McAfee® Email Security Virtual Appliance 5.6

Installationshandbuch

COPYRIGHT

Copyright © 2011 McAfee, Inc. Alle Rechte vorbehalten.

Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übermittelt, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD sind eingetragene Marken oder Marken von McAfee, Inc. und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum der jeweiligen Besitzer.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einführung in die McAfee E-Mail Security Virtual Appliance 5

Einführung in die Funktionen der virtuellen Appliance 5

Verwendung dieses Handbuchs 9

Zielgruppe dieses Handbuchs 9

Umfang des Download-Pakets für die virtuelle Appliance 9

Graphische Konventionen 10

Dokumentation 10

Verfügbare Ressourcen 10

Vorbereitung für die Installation der Virtual Appliance 12

Punkte, die Sie vor der Installation der virtuellen Appliance bedenken sollten 12

Benötigte Netzwerkangaben 12

Betriebsmodi und wie sie Netzwerkverbindungen beeinflussen 13

Modus "Expliziter Proxy" 13

Netzwerk- und Gerätekonfiguration 13

Protokolle 14

Firewall-Regeln 14

Platzieren des Geräts 14

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ 15

SMTP-Konfiguration in einer DMZ 16

E-Mail-Relay 16

E-Mail-Gateway 17

Arbeitslastverwaltung 18

Systemanforderungen 18

Beispiel-Installationsszenarien 19

Ausführen der virtuellen Appliance als einzige virtuelle Maschine auf dem Host 19

Ausführen der virtuellen Appliance zusammen mit anderen virtuellen Maschinen 19

Installieren der virtuellen Umgebung 21

Übersicht über den Installationsvorgang der virtuellen Appliance 21

Bewährte Vorgehensweisen für die Installation 21

Herunterladen der Software für die virtuelle Appliance 22

Installieren der virtuellen Appliance auf VMware vSphere und VMware vSphere Hypervisor (ESXi) 23

Leistungsoptimierung auf VMware vSphere 24
Installieren der virtuellen Appliance auf VMware ESX oder VMware ESXi 25
Vorstellung der Benutzeroberfläche 28
Die Benutzeroberfläche. 28
Dashboard-Statusinformationen und Konfigurationsoptionen. 30
Testen der Konfiguration der Virtual Appliance. 36
Testen der Verbindung. 36
Aktualisieren der DAT-Dateien. 36
Testen von E-Mail-Verkehr und Virenerkennung. 37
Testen der Spam-Erkennung. 37
Funktionen der Virtual Appliance. 38
Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk. 38
Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln. 38
Vermeiden des Verlusts vertraulicher Daten. 41
Bearbeiten von isolierten Nachrichten. 41
Überwachen der Spam-Erkennung. 42
Steuern des Benutzerzugriffs auf Basis einer Rolle. 43
Zusätzliche Konfigurationsoptionen. 44
Aktualisieren auf Email Security Virtual Appliance 5.6. 44
Installieren der virtuellen Appliance auf VMware Server 2.0 unter Microsoft Windows. 45
Installieren der virtuellen Appliance auf VMware Server 1.0 unter Microsoft Windows 47
Ausführen einer virtuellen Appliance auf VMware Server im Betriebsmodus "Transparent". 49
Ausführen einer virtuellen Appliance VMware ESX, VMware vSphere oder VMware ESXi in einem transparenten Betriebsmodus 50
Ändern der standardmäßigen Aktionen zum Ausschalten und Zurücksetzen. 50
Konfigurieren der Optionen zum Herunterfahren und Neustart. 51
Konvertieren von einer VMtrial-Installation. 52
Fehlerbehebung bei der Virtual Appliance. 53
Die Appliance empfängt keinen Datenverkehr aus dem Netzwerk. 53
Probleme mit der Benutzeroberfläche. 54
E-Mail-Probleme. 55
POP3. 56
Probleme bei der physischen Konfiguration. 57
Probleme bei der automatischen Aktualisierung der Antiviren-Software. 57
Probleme mit Anti-Spam. 58

Einführung in die McAfee E-Mail Security Virtual Appliance

Die McAfee® E-Mail Security Virtual Appliance liefert umfassenden Schutz für Unternehmen gegen E-Mail-Bedrohungen in einer integrierten und einfach zu verwaltenden virtuellen Maschine.

Die E-Mail Security Virtual Appliance kann auf den folgenden virtuellen VMware®-Plattformen ausgeführt werden:

- VMware vSphere 4.x und VMware vSphere Hypervisor (ESXi) 4.x
- VMware ESX 3.5 und VMware ESXi 3.5
- VMware Server 2.0 und VMware Server 1.0

Inhalt

- Einführung in die Funktionen der virtuellen Appliance
- Verwendung dieses Handbuchs
- Zielgruppe dieses Handbuchs
- Umfang des Download-Pakets für die virtuelle Appliance
- Graphische Konventionen
- Dokumentation
- Verfügbare Ressourcen

Einführung in die Funktionen der virtuellen Appliance

Diese Informationen beschreiben die Funktionen der McAfee Email Security Virtual Appliance sowie deren Position in der Produktoberfläche:

- Tabelle 1: E-Mail-Scan-Funktionen
- Tabelle 2: Berichterstellungs- und Systemfunktionen

HINWEIS: Im weiteren Verlauf dieses Dokuments finden Sie für einige Funktionen Hinweise zur Verwendung.

Tabelle 1: E-Mail-Scan-Funktionen

Funktion	Beschreibung
Umfassender Scan-Schutz	Die Email Security Virtual Appliance bietet Antiviren- und Anti-Spam-Schutz für die folgenden Netzwerkprotokolle: • SMTP • POP3

Funktion	Beschreibung
Antiviren-Schutz	**E-Mail | E-Mail-Richtlinien | Scan-Richtlinien | [Anti-Virus]** Reduzierung der Bedrohungen für den gesamten Protokollverkehr durch folgende Mittel: • Virenschutzeinstellungen zur Identifizierung bekannter und unbekannter Bedrohungen von Viren in Archivdateien und anderen Dateitypen. • Weitere Einstellungen für die Bedrohungserkennung zum Erkennen von Viren, potentiell unerwünschten Programmen, Komprimierungsprogrammen und anderer Malware. • **Datei-Reputation von McAfee Global Threat Intelligence** zur Ergänzung der DAT-basierten Signaturen, indem den Appliances der Zugriff auf Millionen von Cloud-basierten Signaturen ermöglicht wird. Dadurch wird die Zeitspanne zwischen der Entdeckung einer neuen Malware durch McAfee und deren Aufnahme in die DAT-Dateien reduziert, was den Schutz erhöht.
Anti-Spam-Schutz	**E-Mail | E-Mail-Richtlinien | Scan-Richtlinien | [Spam]** Verringert Spam in SMTP- und POP3-E-Mail-Verkehr durch folgende Mittel: • Anti-Spam-Modul, Anti-Spam- und Anti-Phishing-Regelsätze. • Listen zugelassener und nicht zugelassener Absender • **E-Mail-Reputation von McAfee Global Threat Intelligence** zur Identifizierung von Absendern von Spam-E-Mails. • Einschluss- und Ausschlusslisten, die Administratoren und Benutzer mithilfe eines Microsoft Outlook-Plugins (nur auf Benutzerebene) erstellen können. Erkennt Phishing-Angriffe und ergreift die entsprechenden Maßnahmen.
McAfee Global Threat Intelligence-Feedback	**E-Mail | E-Mail-Richtlinien | Scan-Richtlinien | McAfee GTI-Feedback** **System | Setup-Assistent | Datenverkehr** McAfee analysiert die Daten über Produkterkennungen und -warnmeldungen, Bedrohungsdetails und Nutzerstatistiken von einem vielschichtigen Kundenstamm, um wirksam gegen elektronische Angriffe vorzugehen, anfällige Systeme zu schützen und Internetkriminalität abzuwehren. Durch Ihre Teilnahme am Feedback-Dienst helfen Sie uns dabei, McAfee Global Threat Intelligence zu verbessern, sodass Ihre McAfee-Produkte effektiver arbeiten, und unterstützen unsere Zusammenarbeit mit Strafverfolgungsbehörden im Hinblick auf die Bekämpfung elektronischer Bedrohungen.
Compliance-Einstellungen	**E-Mail | E-Mail-Richtlinien | Scan-Richtlinien | [Compliance]** Diese Version der McAfee Email Security Appliance-Software beinhaltet Verbesserungen hinsichtlich der Art und Weise der Verwendung von Compliance-Regeln: • Verwenden Sie in der **Compliance**-Richtlinie den Assistenten für die Regelerstellung, um die integrierten Wörterbücher für die Compliance-Prüfung festzulegen, oder erstellen Sie eine neue Regel, für die Sie eine vorhandene Regel als Vorlage verwenden können. • Mit den Richtlinien **Mail-Größenfilterung** und **Dateifilterung** können Sie SMTP-E-Mail-Nachrichten auf echte Dateitypen überprüfen und auf der Grundlage der Größe und Anzahl der Anhänge Maßnahmen ergreifen.
Data Loss Prevention	**E-Mail | E-Mail-Richtlinien | Scan-Richtlinien | [Data Loss Prevention]** Mit der **Data Loss Prevention**-Richtlinie können Sie kritische Dokumente hochladen und analysieren – dies wird als "Training" bezeichnet – und einen Fingerabdruck aller Dokumente erstellen.

Funktion	Beschreibung
Nachrichtensuche	**E-Mail | Nachrichtensuche** Mit der Nachrichtensuche können Sie von einer einzigen Stelle der Benutzeroberfläche aus den Status von E-Mails bestätigen, die die Appliance durchlaufen haben. Sie erhalten Informationen zur E-Mail, beispielsweise ob sie zugestellt, blockiert, gebounct, isoliert oder in die Warteschlange für ausstehende weitere Aktionen gestellt wurde.
Quarantänefunktionen	**E-Mail | Quarantäne-Konfiguration | Quarantäneoptionen** • **Quarantäne-Digests** Ermöglichen den Benutzern die Bearbeitung isolierter Elemente ohne Einbeziehung des E-Mail-Administrators. • **McAfee Quarantine Manager** Fasst die Quarantäneverwaltung für McAfee-Produkte zusammen.
Message Transfer Agent	• Leitet Datenverkehr um, basierend auf Kriterien, die vom Administrator festgelegt werden. Beispielsweise können verschlüsselte E-Mails zur Entschlüsselung umgeleitet werden. • Erlaubt es dem Administrator, den finalen Status jeder Nachricht zu bestimmen. • Zeigt eine Kurzübersicht eingehender E-Mails nach Domänen, mit Detaillierungsmöglichkeiten nach Domäne und nicht zugestellter E-Mail nach Domäne. • Priorisiert die erneute Zustellung nicht zugestellter E-Mails abhängig von der Domäne. • Fasst die Zustellung mehrerer E-Mails an die jeweilige Domäne zusammen. • Erneutes Schreiben von E-Mail-Adressen bei ein- und ausgehender E-Mail auf der Grundlage normaler Ausdrücke, die vom Administrator definiert wurden. • Entfernt E-Mail-Header bei ausgehenden Nachrichten, um den Aufbau der internen Netzwerkinfrastruktur zu verbergen. • Versendet E-Mails unter Verwendung von TLS. • Verwaltet Zertifikate.

Tabelle 2: Berichterstellungs- und Systemfunktionen

Funktion	Beschreibung
Geplante Berichte	**Berichte | Geplante Berichte** Sie können Berichte planen, die regelmäßig ausgeführt und an einen oder mehrere E-Mail-Empfänger gesendet werden sollen.
Protokollierungsoptionen	**System | Protokollierung, Warnung und SNMP** Sie können die Appliance für das Senden von E-Mails, die Informationen zu Viren und anderen erkannten Bedrohungen enthalten, sowie für die Verwendung von SNMP zum Übertragen von Informationen von der Appliance konfigurieren.
Dashboard-Statistiken	**Dashboard** Das Dashboard bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Aktivitäten der Appliance ansehen können, wie beispielsweise von der Appliance verarbeitete E-Mails und den Gesamtsystemstatus der Appliance. Sie können auch eine Liste von Links zu Aufgaben konfigurieren, die Sie häufig verwenden.

Funktion	Beschreibung
Verwalten von Appliances über ePolicy Orchestrator	**System | Setup-Assistent | Einrichten der Verwaltung durch ePO** Sie können in ePolicy Orchestrator den Status Ihrer Appliances überwachen und sie verwalten. Sie können die Appliances direkt über ePolicy Orchestrator verwalten, ohne die Benutzeroberfläche für jede Appliance starten zu müssen. In ePolicy Orchestrator ähneln die Seiten der Benutzeroberfläche, die Sie zum Konfigurieren und Verwalten Ihrer Email Security Appliances verwenden, hinsichtlich ihrer Gestaltung den Seiten, die Sie von den Appliances gewohnt sind.
Cluster-Verwaltung	**System | Cluster-Verwaltung** Die Cluster-Verwaltung ermöglicht Ihnen, Gruppen von zusammenarbeitenden Appliances einzurichten, um die Scan-Arbeitslast zu verteilen und für den Fall eines Hardware-Fehlers Redundanz zu bieten. Auf diesen Seiten können Sie Ihre Konfigurationen sichern und wiederherstellen, Konfigurationen von einer Appliance auf andere Appliances übertragen und den Lastenausgleich zwischen den Appliances einrichten.
Virtuelle Hosts	**System | Virtuelles Hosting | Virtuelle Hosts** Für das SMTP-Protokoll können Sie im Adresspool für eingehenden Datenverkehr die Adressen angeben, an denen die Appliance Datenverkehr empfängt oder abfängt. Unter Verwendung virtueller Hosts kann eine einzelne Appliance sich wie verschiedene Appliances verhalten. Jede virtuelle Appliance kann Datenverkehr innerhalb angegebener IP-Adresspools verwalten, wodurch die Appliance Scan-Dienste für Datenverkehr von zahlreichen Kunden bieten kann.
Rollenbasierte Zugriffskontrolle	**System | Benutzer, Gruppen und Dienste | Rollenbasierte Benutzerkonten** Zusätzlich zur Kerberos-Authentifizierungsmethode steht auch die RADIUS-Authentifizierung zur Verfügung.
Internes Rescue-Image	**System | Appliance-Verwaltung | Systemverwaltung | Internes Rescue-Image verwalten** Wenn Sie Ihre Email Security Appliances verwalten, können Sie, wenn das Image für jede Appliance auf einer geschützten Partition auf der Festplatte für jede Appliance gespeichert ist, remote ein neues Image Ihrer Appliances einspielen. Durch das Rescue-Image entfällt die Notwendigkeit, Ihre Appliance mit Karten für den Remote-Zugriff auszustatten (sofern Sie geeignete Appliance-Modelle verwenden), um von einem Remote-Standort aus ein neues Image auf die Appliances einzuspielen. Zusätzlich zur Installation des Software-Images auf der geschützten Partition können Sie auch auf einem USB-Laufwerk ein bootfähiges Image für Ihre Appliances erstellen.

Verwendung dieses Handbuchs

In diesem Handbuch wird Folgendes behandelt:

- Planung und Ausführung Ihrer Installation.
- Umgang mit der Benutzeroberfläche.
- Testen der ordnungsgemäßen Funktion des Produkts.
- Anwendung der aktuellsten Erkennungsdefinitionsdateien.
- Vertrautmachen mit einigen Scan-Richtlinien, Erstellen von Berichten und Abrufen der Statusinformationen.
- Beheben einiger grundlegender Probleme.

Weitere Informationen zu den Scan-Funktionen des Produkts finden Sie in der Online-Hilfe.

Zielgruppe dieses Handbuchs

Dieses Handbuch richtet sich in erster Linie an Netzwerkadministratoren, die für das Virenschutz- und Sicherheitsprogramm ihres Unternehmens verantwortlich sind.

Umfang des Download-Pakets für die virtuelle Appliance

Das Paket für die Email Security Virtual Appliance ist eine ZIP-Datei, die die Installationsdateien für die Software enthält.

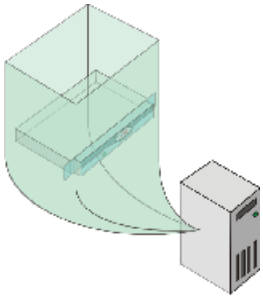
Auf der McAfee-Download-Seite stehen zwei Arten von Paketen zur Verfügung, die Sie abhängig von Ihrer virtuellen Umgebung auswählen:

- Benutzer von vSphere 4.x
- Alle anderen unterstützten VMware-Produkte

HINWEIS: Das Download-Paket enthält keine Installationsdateien für das VMware-Produkt. Wenn Sie Ihre virtuelle Software eingerichtet haben, gehen Sie zur VMware-Website (http://www.vmware.com), um VMware vSphere zu kaufen oder VMware Server oder VMware vSphere Hypervisor (ESXi) herunterzuladen.

Graphische Konventionen

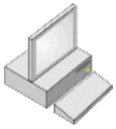
In den Abbildungen dieses Handbuches werden die folgenden Symbole verwendet.



Internet

E-Mail-Server

Anderer Server (z. B. DNS-Server)



Benutzer- oder Client-Computer

Router

Switch

Firewall

Netzwerkzone (DMZ oder VLAN)

Netzwerk

Tatsächlicher Datenpfad

Wahrgenommener Datenpfad

Dokumentation

Dieses Handbuch ist im Lieferumfang Ihres Produkts enthalten. Weitere Informationen finden Sie in der zum Produkt gehörenden Online-Hilfe und der weiteren Dokumentation auf der Website http://mysupport.mcafee.com.

Verfügbare Ressourcen

Hier wird beschrieben, wo Sie weitere Informationen und Hilfe erhalten können.

McAfee-Produkte	McAfee-KnowledgeBase. Gehen Sie zu https://mysupport.mcafee.com/eservice/Default.aspx, und klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen).
VMware-Betriebsumgebung	VMware-Website. Besuchen Sie die Seite http://www.vmware.com/, und klicken Sie in

	der Leiste **Links** auf **Support & Downloads**. Wählen Sie unter **Support Resources** die Option **Knowledge Base**.
Produkthandbuch	McAfee-Download-Site. Enthält Informationen zu grundlegenden Konzepten, Richtlinien, Protokollen (SMTP, POP3), zur Wartung und Überwachung. Sie benötigen Ihre Grant-Nummer.
Online-Hilfe	Produktoberfläche. Enthält Informationen zu grundlegenden Konzepten, Richtlinien, Protokollen (SMTP, POP3), zur Wartung und Überwachung.

Vorbereitung für die Installation der Virtual Appliance

Diese Informationen helfen Ihnen dabei, Ihre Umgebung vorzubereiten, und machen Sie auf Themen aufmerksam, die Sie vor der Installation der McAfee Email Security Virtual Appliance bedenken sollten.

Inhalt

- Punkte, die Sie vor der Installation der virtuellen Appliance bedenken sollten
- Benötigte Netzwerkangaben
- Betriebsmodi und wie sie Netzwerkverbindungen beeinflussen
- Modus "Expliziter Proxy"
- Systemanforderungen

Punkte, die Sie vor der Installation der virtuellen Appliance bedenken sollten

Vor Beginn des Installationsvorgangs sollten Sie Folgendes bedenken:

- Wählen Sie Ihre virtuelle Umgebung: VMware vSphere, VMware vSphere Hypervisor (ESXi) oder VMware Server. Um optimale Leistung und Durchsatz in einer virtuellen Umgebung zu erzielen, empfiehlt McAfee, die virtuelle Appliance auf VMware vSphere auszuführen. VMware Server ist für kleinere Installationen geeignet.
- Verwenden Sie die virtuelle Appliance in Ihrem Unternehmen hinter einer ordnungsgemäß konfigurierten Firewall.
- Die virtuelle Appliance ist kein Mail-Server. Sie müssen die Firewall, den Mail-Server und andere Geräte konfigurieren, um E-Mail-Verkehr zu der virtuellen Appliance zu leiten.
- Sie dürfen zusätzliche Software und Dateien nur dann auf der virtuellen Appliance speichern oder installieren, wenn Sie in der Dokumentation bzw. vom Support-Mitarbeiter dazu aufgefordert werden.
- Die virtuelle Appliance kann nicht alle Arten von Datenverkehr verarbeiten. Der Modus "Expliziter Proxy" kann nur unterstützte Protokolle über die virtuelle Appliance leiten.
- Entscheiden Sie, ob Sie die Out-of-Band-Verwaltungsschnittstelle verwenden möchten.

Benötigte Netzwerkangaben

Ermitteln Sie die folgenden Informationen, um die Konfiguration abzuschließen:

- Zu scannende Protokolle (SMTP, POP3)
- Host-Name
- Domänenname
- Standard-Gateway
- IP-Adresse und Subnetzmaske des LAN1-Anschlusses
- IP-Adresse und Subnetzmaske des LAN2-Anschlusses
- IP-Adresse und Subnetzmaske der Out-of-Band-Verwaltungsschnittstelle
- IP-Adresse des DNS-Servers

Betriebsmodi und wie sie Netzwerkverbindungen beeinflussen

Die McAfee Email Security Virtual Appliance kann in drei Betriebsmodi betrieben werden. Bevor Sie Ihre Appliance installieren und konfigurieren, müssen Sie sich überlegen, welchen Netzwerkmodus Sie verwenden möchten.

Die folgenden Betriebsmodi sind verfügbar:

- Modus "Expliziter Proxy" – Die virtuelle Appliance fungiert als Proxy-Server und Mail-Relay.
- Modus "Transparenter Router" – Die virtuelle Appliance fungiert als Router.
- Modus "Transparente Bridge" – Die virtuelle Appliance fungiert als Ethernet-Bridge.

Der ausgewählte Modus bestimmt, wie Sie die virtuelle Appliance physisch an Ihr Netzwerk anschließen. McAfee empfiehlt, dass Sie die virtuelle Appliance im Modus "Expliziter Proxy" betreiben. Die Einrichtung von virtuellen Appliances, die in einem transparenten Modus betrieben werden, ist schwieriger, ebenso die Wartung in einer virtuellen Umgebung.

Modus "Expliziter Proxy"

Im Modus "Expliziter Proxy" müssen einige Netzwerkgeräte so eingerichtet werden, dass sie Datenverkehr explizit an das Gerät senden. Das Gerät fungiert dann als Proxy oder Relay und verarbeitet den Datenverkehr für die Geräte.

Der Modus "Expliziter Proxy" ist am besten für Netzwerke geeignet, in denen Client-Geräte über ein einzelnes Upstream- und Downstream-Gerät eine Verbindung zum Gerät herstellen.

TIPP: Dies ist möglicherweise nicht die beste Option, wenn verschiedene Netzwerkgeräte erneut konfiguriert werden müssen, damit sie den Datenverkehr an das Gerät senden.

Netzwerk- und Gerätekonfiguration

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet, müssen Sie den internen Mail-Server explizit so konfigurieren, dass er E-Mail-Verkehr an das Gerät sendet. Das Gerät prüft den E-Mail-Verkehr, bevor es ihn im Namen des Absenders an den externen Mail-Server weiterleitet. Der externe E-Mail-Server leitet die E-Mail dann an den Empfänger weiter.

Entsprechend muss das Netzwerk so konfiguriert werden, dass eingehende E-Mail-Nachrichten aus dem Internet nicht dem internen Mail-Server, sondern dem Gerät zugestellt werden.

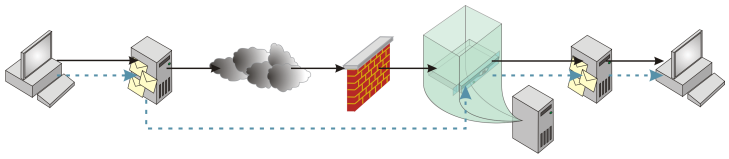


Abbildung 1: Weiterleiten des E-Mail-Verkehrs

Das Gerät kann den E-Mail-Verkehr dann prüfen, bevor es ihn im Namen des Absenders an den internen Mail-Server zur Zustellung weiterleitet, wie in Abbildung 1: Weiterleiten des E-Mail-Verkehrs dargestellt.

Beispielsweise kann ein externer Mail-Server direkt mit dem Gerät kommunizieren, auch wenn der Datenverkehr möglicherweise mehrere Netzwerkserver passiert, bevor er das Gerät erreicht. Der wahrgenommene Pfad verläuft vom externen Mail-Server zum Gerät.

Protokolle

Um ein unterstütztes Protokoll zu scannen, müssen Sie Ihre anderen Netzwerkserver oder Client-Computer so konfigurieren, dass das Protokoll durch das Gerät geleitet wird, sodass kein Datenverkehr das Gerät umgehen kann.

Firewall-Regeln

Im Modus "Expliziter Proxy" werden alle Firewall-Regeln, die für den Client-Zugriff auf das Internet eingerichtet wurden, außer Kraft gesetzt. Für die Firewall sind nur die IP-Adressinformationen für das Gerät sichtbar, nicht die IP-Adressen der Clients. Dies bedeutet, dass die Firewall ihre Internetzugriffsregeln nicht auf die Clients anwenden kann.

Platzieren des Geräts

Konfigurieren Sie die Netzwerkgeräte so, dass der zu scannende Datenverkehr an das Gerät gesendet wird. Das ist wichtiger als der Standort des Geräts.

Der Router muss allen Benutzern erlauben, eine Verbindung zum Gerät herzustellen.

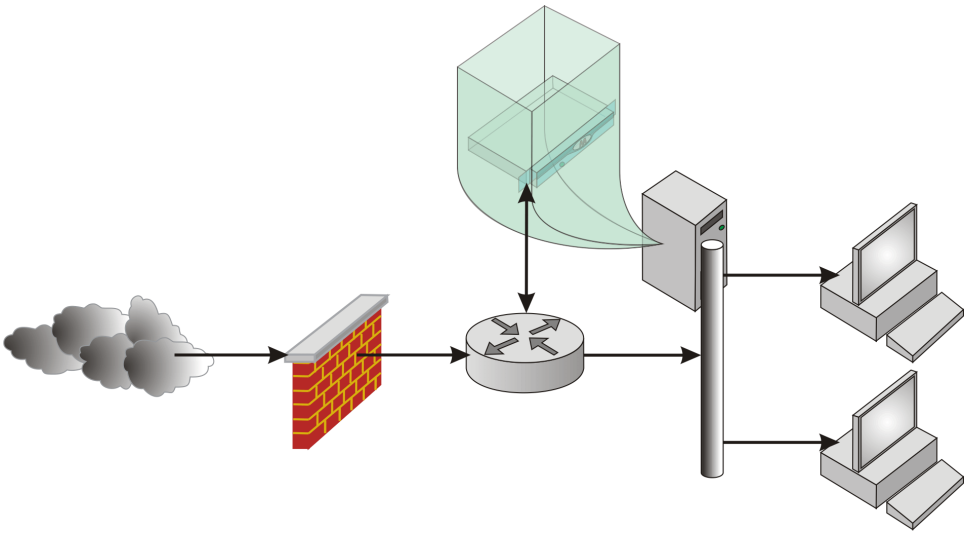


Abbildung 2: Konfiguration als expliziter Proxy

Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall positioniert werden, wie in Abbildung 2: Konfiguration als expliziter Proxy dargestellt.

Normalerweise ist die Firewall so konfiguriert, dass der Datenverkehr, der nicht direkt von dem Gerät stammt, gesperrt wird.

Wenn Sie in Bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkspezialisten.

Verwenden Sie diese Konfiguration in folgenden Fällen:

- Das Gerät wird im Modus "Expliziter Proxy" betrieben.
- Sie verwenden E-Mail (SMTP).

Für diese Konfiguration gilt:

- Konfigurieren Sie die externen DNS-Server (Domain Name System) oder NAT (Network Address Translation) auf der Firewall so, dass der externe Mail-Server E-Mails an das Gerät zustellt, nicht an den internen Mail-Server.
- Konfigurieren Sie die internen Mail-Server so, dass E-Mail-Verkehr an das Gerät gesendet wird. Das heißt, die internen Mail-Server müssen das Gerät als Smart-Host verwenden. Vergewissern Sie sich, dass die Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.
- Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr von dem Gerät akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt. Richten Sie Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ

Eine "demilitarisierte Zone" (Demilitarized Zone, DMZ) ist ein Netzwerk, das durch eine Firewall von allen anderen Netzwerken getrennt ist, auch vom Internet und anderen internen Netzwerken.

Eine DMZ wird üblicherweise mit dem Ziel implementiert, den Zugriff auf Server zu sperren, die Internetdienste (beispielsweise E-Mail) zur Verfügung stellen.

Hacker verschaffen sich oft Zugriff auf Netzwerke, indem sie herausfinden, auf welchen TCP-/UDP-Ports Appliances Anfragen erwarten, und dann bekannte Schwachstellen in Appliances ausnutzen. Firewalls senken das Risiko solcher Exploits erheblich, indem sie den Zugriff auf bestimmte Ports auf bestimmten Servern steuern.

Das Gerät kann einfach zu einer DMZ-Konfiguration hinzugefügt werden. Die Art, wie Sie das Gerät in einer DMZ verwenden, hängt von den zu scannenden Protokollen ab.

Inhalt

- Arbeitslastverwaltung

SMTP-Konfiguration in einer DMZ

Die DMZ ist eine gute Möglichkeit für das Verschlüsseln von E-Mails. Wenn der E-Mail-Verkehr die Firewall zum zweiten Mal erreicht (auf seinem Weg von der DMZ zum internen Netzwerk), ist er verschlüsselt.

Geräte, die SMTP-Verkehr in einer DMZ scannen können, sind normalerweise im Modus "Expliziter Proxy" konfiguriert.

Konfigurationsänderungen müssen nur an den MX-Einträgen für die E-Mail-Server vorgenommen werden.

HINWEIS: Sie können den Modus "Transparente Bridge" verwenden, wenn Sie SMTP in einer DMZ scannen. Wenn Sie jedoch den Datenfluss nicht richtig steuern, scannt das Gerät jede Nachricht zweimal, einmal in jede Richtung. Aus diesem Grund wird für SMTP-Scans normalerweise der Modus "Expliziter Proxy" verwendet.

- E-Mail-Relay
- E-Mail-Gateway

E-Mail-Relay

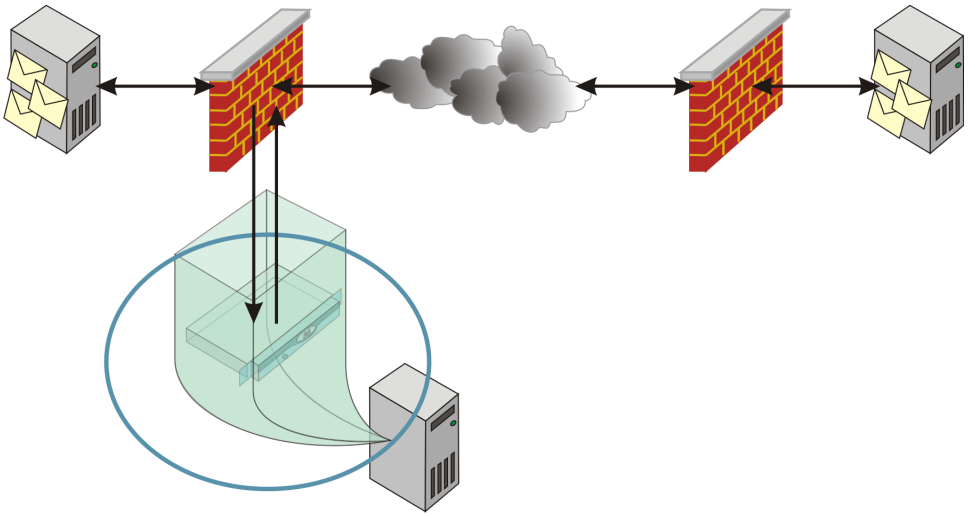


Abbildung 3: Konfiguration eines Geräts im Modus "Expliziter Proxy" in einer DMZ

Wenn Sie in Ihrer DMZ bereits ein Relay eingerichtet haben, können Sie es durch das Gerät ersetzen.

Um Ihre bestehenden Firewall-Richtlinien zu verwenden, geben Sie dem Gerät dieselbe IP-Adresse wie dem Mail-Relay.

E-Mail-Gateway

SMTP bietet keine Methoden zur Verschlüsselung von E-Mail-Nachrichten. Sie können mithilfe von TLS (Transport Layer Security) den Link verschlüsseln, nicht jedoch die E-Mail-Nachrichten. Daher erlauben einige Unternehmen solchen Datenverkehr nicht in ihrem internen Netzwerk. Zur Umgehung dieses Problems wird häufig ein proprietäres E-Mail-Gateway eingesetzt, zum Beispiel Lotus Notes® oder Microsoft® Exchange, um den E-Mail-Datenverkehr zu verschlüsseln, bevor er das interne Netzwerk erreicht.

Um eine DMZ-Konfiguration unter Verwendung des proprietären E-Mail-Gateways zu implementieren, fügen Sie das Scan-Gerät zur DMZ auf der SMTP-Seite des Gateways hinzu.

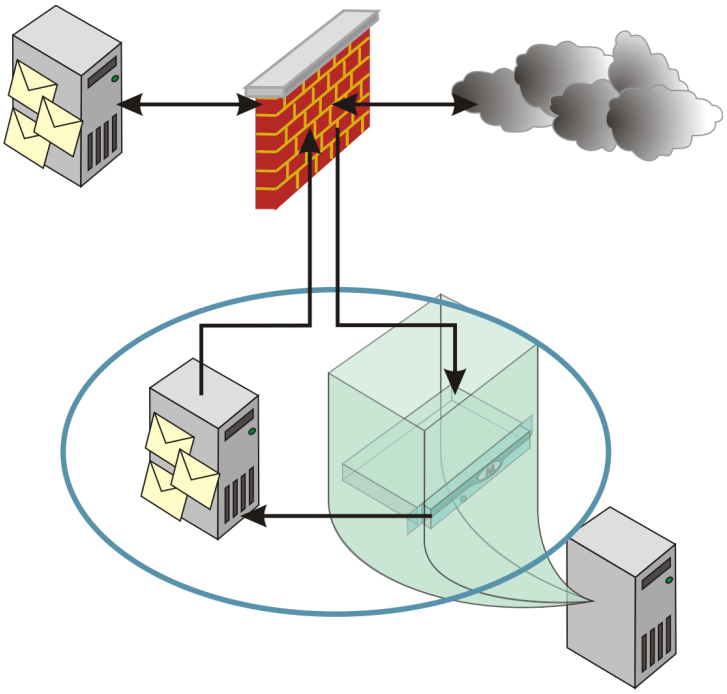


Abbildung 4: Schützen eines E-Mail-Gateways in einer DMZ

Nehmen Sie hierfür folgende Konfigurationen vor:

- Die öffentlichen MX-Einträge müssen externe Mail-Server anweisen, alle eingehenden E-Mail-Nachrichten an das Gerät (statt an das Gateway) zu senden.
- Das Gerät muss alle eingehenden E-Mail-Nachrichten an das Mail-Gateway und alle ausgehenden Nachrichten per DNS oder über ein externes Relay senden.
- Das E-Mail-Gateway muss alle eingehenden E-Mails an die internen Mail-Server und aller andere (ausgehenden) Mails an das Gerät weiterleiten.
- Die Firewall erlaubt nur eingehende E-Mails, die sich an das Gerät richten.

HINWEIS: Bei Firewalls, auf denen die Verwendung von NAT (Network Address Translation) konfiguriert ist und die eingehende E-Mails an die internen E-Mail-Server umleiten, müssen die öffentlichen MX-Einträge nicht neu konfiguriert werden. Sie leiten den Datenverkehr bereits an

die Firewall und nicht an das eigentliche E-Mail-Gateway. In diesem Fall muss die Firewall neu konfiguriert werden, sodass eingehende Nachrichten an das Gerät geleitet werden.

Arbeitslastverwaltung

Die virtuelle Appliance verfügt über eine eigene interne Arbeitslastverwaltung, durch die die Scan-Last gleichmäßig auf alle für die Zusammenarbeit konfigurierten Appliances verteilt wird.

Sie müssen keinen separaten externen Lastenausgleicher bereitstellen.

Systemanforderungen

Stellen Sie sicher, dass Ihr Host-Computer die Systemanforderungen für die von Ihnen gewählte virtuelle VMware-Umgebung erfüllt.

HINWEIS: Besuchen Sie die VMware-Website http://www.vmware.com, um die Systemanforderungen für Ihr VMware-Produkt abzurufen.

Darüber hinaus sollten Sie sicherstellen, dass die virtuelle Maschine, auf der Sie die McAfee Email Security Virtual Appliance ausführen werden, die folgenden minimalen Systemanforderungen erfüllt:

Option	Beschreibung
Prozessor	Zwei virtuelle Prozessoren
Verfügbarer virtueller Speicher	2 GB
Freier Festplattenspeicher	80 GB

HINWEIS: Die Oberfläche der Appliance ist für Microsoft Internet Explorer 7.0 oder höher und Mozilla Firefox 3.5 oder höher optimiert.

Beispiel-Installationsszenarien

In diesem Abschnitt enthalten Sie Informationen zur Installation der virtuellen Appliance in unterschiedlichen Server-Konfigurationen.

Ausführen der virtuellen Appliance als einzige virtuelle Maschine auf dem Host

Diese Informationen zeigen eine mögliche Ausbringung der virtuellen Appliance auf einem einzelnen Server der von Ihnen gewählten virtuellen VMware-Umgebung. VMware ESX, VMware vSphere oder VMware ESXi sind dedizierte Server für die virtuelle Appliance. Deren Hardware-Spezifikation muss die minimalen Hardware-Anforderungen erfüllen, die in den *Richtlinien zu den Email and Web Security-Leistungsdaten* dargelegt sind.

Um mehrere virtuelle Maschinen zu verwalten, die auf einem einzigen VMware-Server ausgeführt werden, lesen Sie die Informationen unter Ausführen der virtuellen Appliance zusammen mit anderen virtuellen Maschinen.

HINWEIS: In diesem Beispiel wird davon ausgegangen, dass Sie die virtuelle Appliance im empfohlenen Modus "Expliziter Proxy" betreiben.

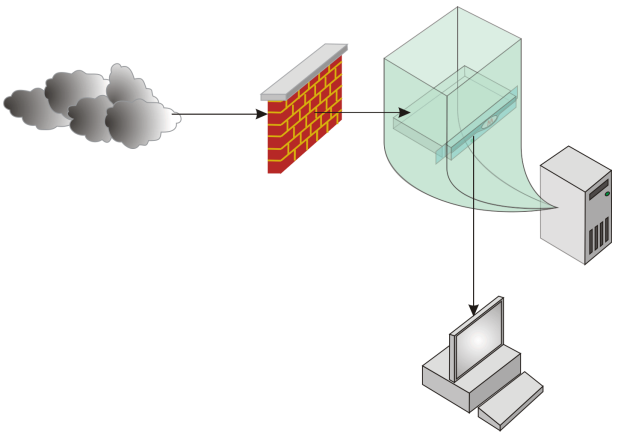


Abbildung 5: Beispiel für eine Installation auf nur einem Server

Ausführen der virtuellen Appliance zusammen mit anderen virtuellen Maschinen

Diese Informationen zeigen die Ausbringung der McAfee Email Security Virtual Appliance auf VMware ESX, VMware vSphere oder VMware ESXi neben anderen virtuellen Maschinen. In diesem Beispiel ist ein VMware-Host für die virtuelle Appliance sowie auch für andere virtuelle

Maschinen verantwortlich, die alle auf derselben Hardware ausgeführt werden. Auf der VMware-Website http://www.vmware.com finden Sie Informationen zum Aufbau eines Ressourcen-Pools für die virtuelle Appliance. Dem Ressourcen-Pool müssen außerdem die Mindestanforderungen an CPU und Arbeitsspeicher zugewiesen sein, wie sie in den *Richtlinien zu den Email and Web Security-Leistungsdaten* dargelegt sind.

HINWEIS: In diesem Beispiel wird davon ausgegangen, dass Sie die virtuelle Appliance im empfohlenen Modus "Expliziter Proxy" betreiben.

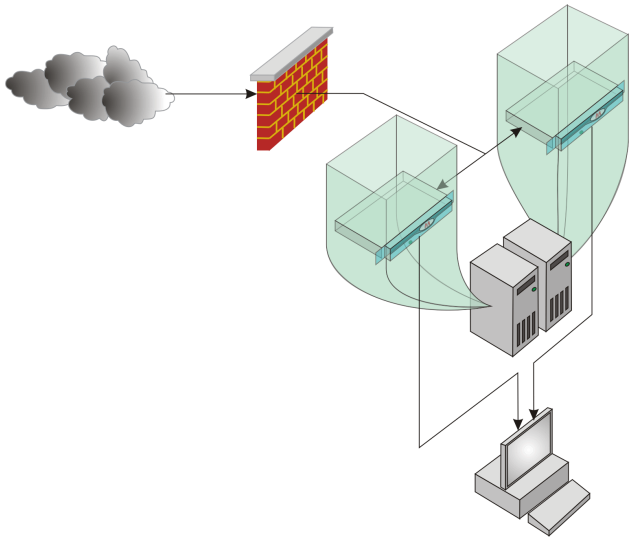


Abbildung 6: Beispiel für eine Installation auf mehreren Servern

Installieren der virtuellen Umgebung

Diese Informationen helfen Ihnen dabei, die virtuelle Umgebung einzurichten und die McAfee Email Security Virtual Appliance darauf zu installieren.

Inhalt

- Übersicht über den Installationsvorgang der virtuellen Appliance
- Bewährte Vorgehensweisen für die Installation
- Herunterladen der Software für die virtuelle Appliance
- Installieren der virtuellen Appliance auf VMware vSphere und VMware vSphere Hypervisor (ESXi)
- Installieren der virtuellen Appliance auf VMware ESX oder VMware ESXi

Übersicht über den Installationsvorgang der virtuellen Appliance

McAfee empfiehlt, dass Sie die Email Security Virtual Appliance in der folgenden Reihenfolge installieren:

1. Installieren Sie das gewünschte VMware-Produkt.
2. Laden Sie die Email Security Virtual Appliance-Installationsdateien herunter.
3. Installieren Sie die virtuelle Appliance in der virtuellen Umgebung.
4. Führen Sie die Konfiguration mithilfe des grafischen Konfigurationsassistenten durch.
5. Melden Sie sich an der virtuellen Appliance an.
6. Testen Sie die Konfiguration.
7. Aktivieren Sie Protokolle.

Bewährte Vorgehensweisen für die Installation

Diese Informationen geben Ihnen einige wichtige Anhaltspunkte für Ihre Installation auf VMware ESX Server, VMware vSphere und VMware ESXi.

HINWEIS: McAfee empfiehlt, dass Sie diese Informationen lesen und berücksichtigen, *bevor* Sie den Installationsprozess starten.

- Die McAfee Email Security Virtual Appliance ist am einfachsten einzurichten und zu warten, wenn sie im standardmäßigen Betriebsmodus "Expliziter Proxy" betrieben wird.
- Machen Sie sich mit den Informationen zum Erstellen von Clustern und Ressourcen-Pools vertraut. Siehe die VMware-Website http://www.vmware.com.

- Verwenden Sie ein Storage Area Network (SAN) statt eines Network File System (NFS), um optimale Ergebnisse zu erzielen.
- Wenn Sie eine Email Security Virtual Appliance in einem der transparenten Modi ausführen:
  - Die Funktionen VMware Distributed Resource Scheduler (DRS) und High Availability (HA) können zu Netzwerkunterbrechungen führen, wenn ein Failover stattfindet.
  - Stellen Sie sicher, dass die Netzwerkkarten der virtuellen Appliance nicht mit derselben Broadcast-Domäne verbunden sind und dass sich die IP-Adressen nicht in demselben Subnetz befinden, um Netzwerk-Loops zu vermeiden.
  - Stellen Sie sicher, dass jeder Netzwerkadapter auf der virtuellen Appliance mit einem anderen physischen Netzwerk auf dem Host-Computer verbunden ist.
  - Sie benötigen mindestens drei Netzwerkkarten im VMware-Host. Die virtuelle Appliance benötigt zwei Netzwerkkarten. VMware empfiehlt eine dedizierte Netzwerkkarte für die Service-Konsole.

Herunterladen der Software für die virtuelle Appliance

Gehen Sie wie nachfolgend beschrieben vor, um die McAfee Email Security Virtual Appliance-Software herunterzuladen. Wir stellen die Software als ZIP-Datei auf der McAfee-Download-Website zur Verfügung.

Vorbereitung

- Lesen Sie das Installationshandbuch zu Ihrem VMware-Produkt.
- Suchen Sie nach der McAfee-Grant-Nummer, die Sie beim Kauf der virtuellen Appliance erhalten haben.

Vorgehensweise

1. Gehen Sie zur McAfee-Website http://www.mcafee.com. Halten Sie den Mauszeiger über Ihren Geschäftstyp, und klicken Sie auf **Downloads**.
2. Klicken Sie auf der Seite **Meine Produkte – Downloads** auf **Anmelden**.
3. Geben Sie die McAfee-Grant-Nummer ein, die Sie beim Kauf der virtuellen Appliance erhalten haben, und klicken Sie auf **Senden**.
4. Wählen Sie aus der Produktliste **Email and Web Security**.
5. Akzeptieren Sie die Lizenzbedingungen, wählen Sie die neueste ZIP-Datei, und laden Sie sie herunter.

   HINWEIS: McAfee empfiehlt, dass Sie die Versionsinformationen lesen, die Sie mit der virtuellen Appliance erhalten haben, bevor Sie die Installation fortsetzen.

Installieren der virtuellen Appliance auf VMware vSphere und VMware vSphere Hypervisor (ESXi)

Gehen Sie wie nachfolgend beschrieben vor, um McAfee Email Security Virtual Appliance auf einem Host-Computer zu installieren, auf dem VMware vSphere 4 oder VMware vSphere Hypervisor (ESXi) 4.0 ausgeführt wird.

Wenn Sie das Produkt Email Security Appliance (VMtrial) verwendet haben, um die Software zu testen, können Sie Ihre VMtrial-Konfiguration speichern und auf der virtuellen Appliance wiederherstellen, wenn die Installation abgeschlossen ist.

Vorbereitung

- Laden Sie die VMware vSphere-Version der Paket-ZIP-Datei von der McAfee-Download-Website herunter, und extrahieren Sie sie an einen Speicherort, auf den der VMware vSphere Client zugreifen kann.
- Installieren Sie eine lizenzierte Vollversion von VMware vSphere 4 oder VMware vSphere Hypervisor (ESXi) 4.0.

Vorgehensweise

1. Starten Sie die VMware vSphere Client-Anwendung.
2. Melden Sie sich beim VMware vSphere-Server oder dem vCenter Server an.
3. Wählen Sie aus der Liste **Inventory** (Inventar) den Host oder Cluster, auf dem Sie die Email Security Virtual Appliance-Software importieren möchten.
4. Klicken Sie auf **File | Deploy OVF Template | Deploy From File** (Datei | OVF-Vorlage bereitstellen | Aus Datei bereitstellen), klicken Sie auf **Browse** (Durchsuchen), und navigieren Sie zu dem Speicherort, an dem Sie die von der McAfee-Download-Seite heruntergeladene ZIP-Datei extrahiert haben.
5. Wählen Sie die Datei **EWS-SMG-<Build-Nummer>.VMbuy.ova**, und klicken Sie auf **Open** (Öffnen).
6. Klicken Sie zwei Mal auf **Next** (Weiter), und geben Sie optional einen neuen Namen ein.
7. Wählen Sie einen Ressourcen-Pool aus, sofern Sie einen konfiguriert haben.
8. Wählen Sie den Datenspeicher aus, und klicken Sie auf **Next** (Weiter).
9. Wählen Sie die virtuellen Netzwerke aus, mit denen die Netzwerkkarten der virtuellen Appliances verbunden werden.
10. Klicken Sie auf **Next** (Weiter), lesen Sie die Zusammenfassung, klicken Sie anschließend auf **Finish** (Fertig stellen), und warten Sie, bis der Importvorgang beendet ist.
11. Starten Sie die virtuelle Appliance. Die Installation beginnt automatisch.
12. Lesen Sie die Endbenutzer-Lizenzvereinbarung, um die Installation fortzusetzen, und klicken Sie dann auf **j**, um sie zu akzeptieren und mit der Installation zu beginnen.
13. Wählen Sie beim Installationsmenü **1** aus, um eine vollständige Installation auszuführen, und **j**, um fortzufahren.
14. Nachdem die Installation abgeschlossen ist, wird die virtuelle Appliance neu gestartet.
15. Wählen Sie im Eröffnungsfenster der Email Security Virtual Appliance die Sprache aus, die Sie verwenden möchten.
16. Stimmen Sie den Bedingungen des Lizenzvertrags zu.

17 Konfigurieren Sie die Email Security Virtual Appliance mithilfe des grafischen Konfigurationsassistenten.

HINWEIS: McAfee empfiehlt, dass Sie die virtuelle Appliance im standardmäßigen Modus "Expliziter Proxy" betreiben.

18 Übernehmen Sie die Konfiguration auf die virtuelle Appliance. In Abhängigkeit von den eingegebenen Einstellungen wird möglicherweise ein Neustart durchgeführt. Sie können die virtuelle Appliance auf mehr als einem VMware ESX-Server oder VMware ESXi-Server installieren. Gehen Sie dazu folgendermaßen vor:

a Führen Sie die Schritte in dieser Aufgabe auf einem anderen VMware ESX-Server oder VMware ESXi-Server aus.

b Kehren Sie zur Benutzeroberfläche der zuvor installierten virtuelle Appliance zurück.

c Gehen Sie zu **System | Cluster-Verwaltung | Konfigurations-Push**, um die Konfigurationsdetails an die zweite virtuelle Appliance zu senden.

Leistungsoptimierung auf VMware vSphere

Mithilfe der folgenden Schritte können Sie möglicherweise die Systemleistung in VMware vSphere-Umgebungen steigern, indem Sie die Standardeinstellungen für Festplatten, Netzwerkadapter, Arbeitsspeicher und CPU ändern.

Vorgehensweise

1 So bearbeiten Sie die Festplatteneinstellungen:

a Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist.

b Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance in der Liste **Inventory** (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).

Im Dialogfeld **Virtual Machine Properties** (Eigenschaften der virtuellen Maschine) befinden sich drei Festplatten, die der virtuellen Appliance zur Verfügung stehen:

- **Hard disk 1** (Festplatte 1) enthält die Installationsdateien der virtuellen Appliance und darf weder entfernt noch verändert werden.
- **Hard disk 2** (Festplatte 2) ist die Hauptfestplatte, die von der virtuellen Appliance verwendet wird. Sie können deren Größe verändern, McAfee empfiehlt jedoch, sie nicht zu verkleinern.
- **Hard disk 3** (Festplatte 3) enthält den temporären Swap-Speicher der virtuellen Appliance.

HINWEIS: Die Leistung kann möglicherweise erhöht werden, indem die zweite und die dritte Festplatte auf zwei getrennten Datenspeichern abgelegt werden.

2 So ändern Sie die Netzwerkadaptereinstellungen:

a Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist.

b Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance in der Liste **Inventory** (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).

c Wählen Sie im Dialogfeld **Virtual Machine Properties** (Eigenschaften der virtuellen Maschine) **Network adapter 1** (Netzwerkadapter 1), und klicken Sie auf **Remove** (Entfernen).

d Wiederholen Sie dies für Adapter 2 und 3.

e Klicken Sie auf **Add** (Hinzufügen).

f Wählen Sie **Ethernet Adapter** (Ethernet-Adapter), und klicken Sie auf **Next** (Weiter).

g Wählen Sie unter **Adapter Type** (Adaptertyp) die Option **VMXNET 3**.

h Wählen Sie das benannte Netzwerk aus, an das Sie LAN1 der virtuellen Appliance anschließen möchten, und stellen Sie sicher, dass die Option **Connect at power on** (Beim Einschalten verbinden) ausgewählt ist.

i Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertig stellen).

j Wiederholen Sie die Schritte e bis i für die Netzwerkadapter 2 und 3.

HINWEIS: Netzwerkadapter 2 wird mit dem Anschluss LAN2 der virtuellen Appliance verbunden. Der dritte Adapter wird für die Out-of-Band-Verwaltung verwendet.

3 So bearbeiten Sie die Einstellungen für Arbeitsspeicher und virtuelle CPU:

a Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist.

b Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance in der Liste **Inventory** (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).

c Ändern Sie im Dialogfeld **Virtual Machine Properties** (Eigenschaften der virtuellen Maschine) die Einstellungen nach Bedarf.

HINWEIS: McAfee empfiehlt, dass Sie die Einstellungen nicht auf weniger als die Standardeinstellungen oder die empfohlenen Systemanforderungen für die virtuelle Appliance herabsetzen.

Installieren der virtuellen Appliance auf VMware ESX oder VMware ESXi

Gehen Sie wie nachfolgend beschrieben vor, um die McAfee Email Security Virtual Appliance auf einem Host-Computer zu installieren, auf dem VMware ESX 3.5 oder VMware ESXi ausgeführt wird.

Wenn Sie das Produkt Email Security Appliance (VMtrial) verwendet haben, um die Software zu testen, können Sie Ihre VMtrial-Konfiguration speichern und auf der virtuellen Appliance wiederherstellen, wenn die Installation abgeschlossen ist.

Vorbereitung

- Laden Sie die ZIP-Datei des Pakets, das die Installationsdateien für VMware ESX und VMware Server enthält, von der McAfee-Download-Seite herunter, und extrahieren Sie sie an einem Speicherort, auf den der VMware Virtual Infrastructure Client Zugriff hat.
- Installieren Sie eine lizenzierte Vollversion von VMware ESX Server 3.5 oder VMware ESXi.

Vorgehensweise

1 Starten Sie die Anwendung VMware Virtual Infrastructure Client.

2 Melden Sie sich beim VMware ESX-Server, VMware ESXi oder dem Virtual Center Server an.

3 Wählen Sie aus der Liste **Inventory** (Inventar) den VMware ESX-Server oder den VMware ESXi-Server, auf den Sie die Email Security Virtual Appliance-Software importieren möchten.

4 Klicken Sie auf der Registerkarte **Getting Started** (Erste Schritte) auf **Import Virtual Appliance** (Virtuelle Appliance importieren), und wählen Sie **Import from file** (Aus Datei importieren).

5 Klicken Sie auf **Browse** (Durchsuchen), um zu dem Speicherort zu wechseln, an den Sie die ZIP-Datei extrahiert haben, die Sie von der McAfee-Download-Website heruntergeladen haben.

6 Öffnen Sie den Unterordner **McAfee-EWS-SMG-<Build-Nummer>.VMbuy-OVF**, wählen Sie **McAfee-EWS-SMG-<Build-Nummer>.VMbuy.OVF**, und klicken Sie auf **Öffnen**.

7 Klicken Sie zwei Mal auf **Next** (Weiter), und geben Sie optional einen neuen Namen ein.

8 Klicken Sie auf **Next** (Weiter).

9 Wenn Sie den Virtual Center Server verwenden, wählen Sie den Datenspeicher aus, den Sie verwenden möchten, und klicken Sie auf **Next** (Weiter). Wenn Sie den Virtual Infrastructure Client verwenden, fahren Sie einfach mit dem nächsten Schritt fort.

10 Wählen Sie die virtuellen Netzwerke aus, mit denen die Netzwerkkarten der virtuellen Appliance verbunden werden.

- **Network 1** – LAN 1
- **Network 2** – LAN 2
- **Network 3** – Out-of-Band-Verwaltungsschnittstelle

HINWEIS: Navigieren Sie nach der Installation in der Benutzeroberfläche des Produkts zu **System | Appliance-Verwaltung | Remote-Zugriff**, um zu den Einstellungen für die Out-of-Band-Verwaltung zu gelangen.

11 Klicken Sie auf **Next** (Weiter), lesen Sie die Zusammenfassung, klicken Sie anschließend auf **Finish** (Fertig stellen), und warten Sie, bis der Importvorgang beendet ist.

HINWEIS: Sie können die standardmäßigen Einstellungen für **Memory** (Arbeitsspeicher), **Hard Disk** (Festplatte) und **Virtual CPU** (Virtuelle CPU) für die virtuelle Appliance ändern. Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist. Wählen Sie anschließend die virtuelle Appliance aus der Liste **Inventory** (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten). *McAfee empfiehlt, diese Einstellungen nicht unter die Standardeinstellungen oder die empfohlenen Systemanforderungen für die virtuelle Appliance herabzusetzen.*

12 Starten Sie die virtuelle Appliance, und wählen Sie **Connect CD/DVD1** (CD/DVD1 verbinden) aus. Stellen Sie dann eine Verbindung zum ISO-Image her.

13 Wechseln Sie zu dem Speicherort, an den Sie die ZIP-Datei für die Email Security Virtual Appliance extrahiert haben. Wählen Sie die ISO-Datei aus, und klicken Sie dann auf **Open** (Öffnen), um das CD-ROM-Laufwerk mit der ISO-Datei zu verbinden.

14 Klicken Sie in das Konsolenfenster, um den Mauszeiger wieder zu aktivieren.

15 Warten Sie auf die Meldung "Operating System not found" (Betriebssystem nicht gefunden), und drücken Sie dann die ESC-Taste, um das CD-ROM-ISO-Image zu starten.

16 Lesen Sie die Endbenutzer-Lizenzvereinbarung, um die Installation fortzusetzen, und geben Sie dann **j** ein, um sie zu akzeptieren und mit der Installation zu beginnen.

17 Wählen Sie beim Installationsmenü **1** aus, um eine vollständige Installation auszuführen, und **j**, um fortzufahren.

18 Nachdem die Installation abgeschlossen ist, wird die virtuelle Appliance neu gestartet.

McAfee empfiehlt, nach Abschluss der Installation das ISO-Image von der CD-ROM zu trennen. Wählen Sie zu diesem Zweck die Option **Disconnect CD/DVD1** (CD/DVD1 trennen).

19 Wählen Sie im Eröffnungsfenster der Email Security Virtual Appliance die Sprache aus, die Sie verwenden möchten.

20 Stimmen Sie den Bedingungen des Lizenzvertrags zu.

21 Konfigurieren Sie die Email Security Virtual Appliance mithilfe des grafischen Konfigurationsassistenten.

HINWEIS: McAfee empfiehlt, dass Sie die virtuelle Appliance im standardmäßigen Modus "Expliziter Proxy" betreiben.

22 Übernehmen Sie die Konfiguration auf die virtuelle Appliance. In Abhängigkeit von den eingegebenen Einstellungen wird möglicherweise ein Neustart durchgeführt. Sie können die virtuelle Appliance auf mehr als einem VMware ESX-Server oder VMware ESXi-Server installieren. Gehen Sie dazu folgendermaßen vor:

a Führen Sie die Schritte in dieser Aufgabe auf einem anderen VMware ESX-Server oder VMware ESXi-Server aus.

b Kehren Sie zur Benutzeroberfläche der zuvor installierten virtuelle Appliance zurück.

c Gehen Sie zu **System | Cluster-Verwaltung | Konfigurations-Push**, um die Konfigurationsdetails an die zweite virtuelle Appliance zu senden.

Vorstellung der Benutzeroberfläche

Diese Informationen geben Auskunft über die Benutzeroberfläche der McAfee Email Security Virtual Appliance und die Seite "Dashboard".

Inhalt

- Die Benutzeroberfläche
- Dashboard-Statusinformationen und Konfigurationsoptionen

Die Benutzeroberfläche

Verwenden Sie diese Informationen, um die Elemente der Benutzerschnittstelle kennenzulernen.

HINWEIS: Ihre Benutzeroberfläche sieht möglicherweise etwas anders als die in Abbildung 7: Das Dashboard gezeigte Oberfläche aus, da sie aufgrund der Hardware-Plattform, Software-Version und Sprache der Appliance variieren kann.

Die Benutzeroberfläche enthält die folgenden Elemente:

- **Navigationsleiste**

  Die Navigationsleiste umfasst vier Bereiche: Benutzerinformationen, Abschnittssymbole, Registerkartenleiste und Support-Steuerelemente.

- **Benutzerinformationsleiste**
- **Abschnittssymbole**

  Die Anzahl der Abschnittssymbole hängen von der verwendeten Software-Version ab. Klicken Sie auf ein Symbol, um die Informationen im Inhaltsbereich und in der Registerkartenleiste zu ändern. Die folgenden Symbole sind verfügbar:

  Tabelle 3: Abschnittselemente

Symbol	Menü	Funktionen
	Dashboard	Auf dieser Seite finden Sie eine Übersicht über die Appliance. Von hier aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern.
	Berichte	Auf den Seiten **Berichte** können Sie Ereignisse sehen, die auf der Appliance aufgezeichnet wurden, wie beispielsweise in E-Mails erkannte Viren und Systemaktivitäten wie etwa Details zu kürzlich erfolgten Aktualisierungen und Anmeldungen.

Symbol	Menü	Funktionen
	E-Mail	Mithilfe der Seiten **E-Mail** können Sie Bedrohungen in E-Mails verwalten, infizierte E-Mails isolieren und weitere Aspekte der E-Mail-Konfiguration behandeln.
	System	Auf den **Systemseiten** können Sie verschiedene Funktionen der Appliance konfigurieren.
	Fehlerbehebung	Auf den Seiten zur **Fehlerbehebung** können Sie sämtliche Probleme im Zusammenhang mit der Appliance analysieren.

- **Registerkartenleiste**

  Die Inhalte der Registerkartenleiste werden durch das ausgewählte Abschnittssymbol bestimmt. Die ausgewählte Registerkarte gibt vor, was im Inhaltsbereich angezeigt wird.

- **Support-Steuerungsschaltflächen**

  Die Support-Steuerungsschaltflächen sind Aktionen, die für den Inhaltsbereich gelten.

  Tabelle 4: Support-Steuerungsschaltflächen

Symbol	Beschreibung
	Aktualisiert den Inhalt.
	Bringt Sie zur zuvor angezeigten Seite zurück. Es wird empfohlen, auf diese Schaltfläche statt auf die Schaltfläche "Zurück" Ihres Browsers zu klicken.
	Dieses Symbol wird angezeigt, wenn Sie etwas konfigurieren, und ermöglicht es Ihnen, Ihre Änderungen anzuwenden.
	Dieses Symbol wird angezeigt, wenn Sie etwas konfigurieren, und ermöglicht es Ihnen, Ihre Änderungen zu verwerfen.
	Öffnet ein Fenster mit Hilfe-Informationen. Viele der Informationen in diesem Fenster finden Sie auch im Produkthandbuch.

- **Steuerelemente anzeigen**

  Die Schaltfläche "Steuerelemente anzeigen" blendet ein Statusfenster ein oder aus.

  Das Statusfenster rechts unten in der Benutzeroberfläche zeigt alle kürzlich erfolgten Aktivitäten an. Neue Meldungen werden oben im Fenster hinzugefügt. Wenn eine Meldung blau und unterstrichen ist, können Sie auf den Link klicken, um eine andere Seite zu besuchen. Sie können das Fenster auch über die Links **Leeren** und **Schließen** verwalten.

- **Inhaltsbereich**

  Der Inhaltsbereich enthält den derzeit aktiven Inhalt. Hier findet die meiste Interaktion statt.

HINWEIS: Die vorgenommenen Änderungen werden wirksam, nachdem Sie auf das grüne Häkchen geklickt haben.

Dashboard-Statusinformationen und Konfigurationsoptionen

Das Dashboard bietet eine Zusammenfassung der Aktivitäten der Appliance.

Von dieser Seite aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern. Auf einer Cluster-Master-Appliance verwenden Sie diese Seite auch, um eine Übersicht der Aktivitäten im Appliance-Cluster anzuzeigen.

HINWEIS: Wenn Sie die Ansicht in einem Bereich ändern möchten, klicken Sie auf **Bearbeiten**, um ein anderes Fenster zu öffnen.

Das Dashboard bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Aktivitäten der Appliance ansehen können.

Abhängig davon, wie Sie Ihre Appliance konfiguriert haben, können Sie Informationen zu Folgendem ansehen:

- Von der Appliance verarbeitete E-Mails
- Gesamtsystemstatus der Appliance
- Aktuelle Erkennungsraten
- Leistung Ihres Netzwerks
- E-Mail-Nachrichten, die von der Appliance in die Warteschlange gestellt wurden
- Anzahl Ihrer eingerichteten Scan-Richtlinien, nach Protokoll getrennt

Sie können auch eine Liste von Links zu Aufgaben konfigurieren, die Sie häufig verwenden. Dies bietet Ihnen eine schnelle und einfache Methode, um zum richtigen Bereich der Benutzeroberfläche zu navigieren.

Im unteren Bereich dieser Seite werden wichtige grafische Informationen zur Leistung der Appliance angezeigt. Jeder dieser Dashboard-Bereiche kann dahingehend angepasst werden, dass er die Informationen anzeigt, die Sie am häufigsten benötigen.

Wenn Sie sich bei der Appliance anmelden und während der Arbeit auf den Konfigurationsseiten der Appliance wird in der unteren rechten Ecke des Bildschirms ein Dialogfeld angezeigt, das Informationen zu empfohlenen Konfigurationsänderungen oder Warnmeldungen hinsichtlich

des Betriebs oder der Einstellungen der Appliance enthält. Sie werden beispielsweise gewarnt, wenn das Global Threat Intelligence-Feedback nicht für alle Richtlinien aktiviert ist.

Abbildung 7: Das Dashboard

Bereiche der Seite "Dashboard"

Tabelle 5: Dashboard – Optionsbeschreibungen

Option	Beschreibung
E-Mail-Erkennungen	Zeigt die Anzahl der Erkennungen unter jedem Protokoll an. Klicken Sie auf **Bearbeiten**, um die Ansicht in diesem Fenster zu ändern. Obwohl Sie festlegen können, dass zu einem Protokoll keine Informationen angezeigt werden, scannt die Appliance den Verkehr weiterhin.
Systemstatus	Zeigt den Status wichtiger Komponenten an und ermöglicht Ihnen, Änderungen an den Einstellungen von empfohlenen Systemkonfigurationsänderungen vorzunehmen: • Bei **Aktualisierungen** zeigt ein grünes Häkchen, dass die Komponenten automatisch aktualisiert werden. Wenn Sie eine manuelle Aktualisierung vornehmen möchten, klicken Sie auf den blauen Link. • Für andere Komponenten gibt ein grünes Häkchen an, dass die Komponente innerhalb akzeptabler Grenzwerte betrieben wird. Weiterführende Informationen erhalten Sie, wenn Sie auf die blauen Links klicken. • Sie können die Stufen anpassen, bei denen die Warnhinweissymbole angezeigt werden, und ändern, was im Dialogfeld mit den empfohlenen Konfigurationsänderungen angezeigt wird, indem Sie auf **Bearbeiten** klicken.
Aktuelle Erkennungsraten	Zeigt mithilfe von Symbolen den Status wichtiger Erkennungen der Appliance an.
Netzwerk	Zeigt die Anzahl der Verbindungen unter jedem Protokoll an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten**

Option	Beschreibung
	abwählen können, wickelt die Appliance den Verkehr weiterhin ab.
E-Mail-Warteschlangen	Zeigt mithilfe von Symbolen die Anzahl der Elemente und die Anzahl der Empfänger für jedes Element in den Warteschlangen "In der Warteschlange", "Isoliert" und "Anfragen für Entlassen aus Quarantäne" an, die von der Appliance verwaltet werden. Wenn Sie auf die Seiten wechseln möchten, auf denen die Warteschlangen verwaltet werden, klicken Sie auf die blauen Links. Wenn Sie die E-Mails in den Warteschlangen schnell durchsuchen möchten, klicken Sie auf **Schnellsuche**.
Scan-Richtlinien	Zeigt eine Liste der von der Appliance eingesetzten Richtlinien an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** abwählen können, wendet die Appliance weiterhin Richtlinien auf den Verkehr an. Wenn Sie die Scan-Richtlinien anzeigen oder weitere Richtlinien hinzufügen möchten, klicken Sie auf die blauen Links.
Tasks	Zeigt eine Liste häufiger Aufgaben an. Wenn Sie Aufgaben entfernen oder neu organisieren möchten, klicken Sie auf **Bearbeiten**.
Lastenausgleich	Auf einer Master-Cluster-Appliance wird der Status des Appliance-Clusters angezeigt. Um die Einstellungen der Anzeige zu ändern, klicken Sie auf **Bearbeiten**.
Diagramme...	Zeigt Diagramme an, die die zeitliche Aktivität der Appliance darstellen. Obwohl Sie ein Protokoll nach Klicken auf "Bearbeiten" abwählen können, überwacht die Appliance den Verkehr weiterhin.

Lastenausgleich

HINWEIS: Dieser Abschnitt ist nur auf einer Cluster-Master-Appliance oder einem Management-Blade (auf einem Content Security Blade Server) verfügbar.

Tabelle 6: Lastenausgleich – Optionsbeschreibungen

Option	Beschreibung
E-Mail	Wenn Sie hierauf klicken, zeigt die Anzeige Nachrichten pro Stunde (E-Mail) an.
Nachrichten pro Stunde (E-Mail)	Zeigt den durchschnittlichen Durchsatz des Clusters auf der Grundlage der alle paar Minuten vorgenommenen Messungen. Wenn ein Cluster doppelt so viele Scan-Appliances umfasst, verdoppelt sich der Durchsatz fast. Zusätzliche Verwaltungsaktivitäten beanspruchen ebenfalls Verarbeitungsleistung.
Status	Zeigt den Status des Geräts an: • – Normaler Betrieb • – Erfordert Aufmerksamkeit • – Erfordert sofortige Aufmerksamkeit
Typ des Scan-Geräts	Zeigt den Typ des Scan-Geräts an: • – Cluster-Master • – Cluster-Failover

Option	Beschreibung
	• – Email Security Appliance
Name	Zeigt den konfigurierten Namen der Appliance an.
Status	Zeigt den aktuellen Status der einzelnen Appliances an: • **Netzwerk** – Mit dem Netzwerk verbunden. • **Redundant** – Das Cluster-Failover-Gerät arbeitet derzeit nicht, übernimmt jedoch, falls die Master-Cluster-Appliance ausfällt. • **Installieren** – Installieren der Software. • **Synchronisieren** – Synchronisieren mit dem Cluster-Master. • **Starten** – Neustart wird durchgeführt. • **Herunterfahren** – Das Gerät wird heruntergefahren. • **Falsch konfiguriert** – Die Konfigurationsdatei ist fehlerhaft. • **Nicht konfiguriert** – Nicht für den Lastenausgleich konfiguriert. • **Deaktiviert** – Durch den Benutzer deaktiviert. • **Fehlgeschlagen** – Nicht mehr im Netzwerk. Es wurde kein "Heartbeat" erkannt. • **Fehler** – Auf dieser Appliance wurde ein Fehler festgestellt. • **Frühere Version** – Nicht mit dem Lastenausgleich kompatibel.
Auslastung	Zeigt die durchschnittliche Systemauslastung während eines Zeitraums von fünf Minuten an.
Aktiv	Zeigt die Anzahl an aktiven Verbindungen für jede Appliance an. Die Zeile für den Cluster-Master zeigt die Gesamtzahl für alle Appliances an.
Verbindungen	Zeigt die Anzahl an Verbindungen an, die von den einzelnen Appliance verarbeitet wurden, seit die Zähler zum letzten Mal zurückgesetzt wurden.
Informationen zur Komponentenversion	Zeigt die Versionen der Anti-Spam- und Antiviren-DAT-Dateien. Wenn die Appliances auf dem aktuellen Stand sind, stimmen die Versionsnummern überein. Während der Aktualisierung können die Werte voneinander abweichen. Um weitere Informationen anzuzeigen, bewegen Sie den Mauszeiger über den Text, und warten Sie, bis ein gelbes Kästchen angezeigt wird.

Zählerverhalten

Alle Zähler lösen für jede Erkennung einmal aus. Wenn beispielsweise eine Nachricht zwei Anhänge hat, die beide infizierte Inhalte enthalten, wird der **Virenzähler** um zwei erhöht. Die Informationen in der folgenden Tabelle gelten, sofern nicht anders angegeben, für SMTP- und POP3-Statistiken.

Tabelle 7: Zählerverhalten

Zähler	Verhalten
Nachrichten	Der **SMTP-Zähler** wird in folgenden Fällen um eins erhöht: • Wenn eine TCP-Verbindung zum SMTP-Port auf der Appliance hergestellt wird

Zähler	Verhalten
	• Ab dem zweiten <MAIL FROM>-Befehl, wenn mehrere E-Mails in derselben SMTP-Konversation empfangen werden Der **POP3-Zähler** wird für jede Nachricht, die von der Appliance heruntergeladen wird, um eins erhöht.
Sichere Nachrichten	Wird in den folgenden Fällen um eins erhöht: • Wenn ein STARTTLS-Befehl über den Standard-SMTP-Port ausgegeben wird • Wenn die Appliance die TLS-Konversation abfängt, ab dem zweiten <MAIL FROM>-Befehl, wenn mehrere E-Mails in derselben SMTP-Konversation empfangen werden • Wenn Nachrichten über SMTPS gesendet werden
Blockierte Verbindungen	Wird für jedes SYN-Paket um eins erhöht, das von einer IP-Adresse stammt, die eine "Ablehnen, schließen und verweigern (Blockieren)"-Aktion ausgelöst hat. Die RBL-Suchfunktion (Realtime Blackhole List) ist so konfiguriert, dass diese Aktion standardmäßig für die nächsten zehn Minuten ausgeführt wird.
Viren, PUPe, Compliance und Data Loss Prevention	Wird für jede Erkennung um eins erhöht. Wenn beispielsweise eine Nachricht zwei Anhänge hat, die beide infizierte Inhalte enthalten, wird der **Virenzähler** um zwei erhöht.
Spam und Phishing und **Absenderauthentifizierung**	Wird für jede Nachricht, die den Scanner auslöst, um eins erhöht
Sonstige	Wird für jede Erkennung um eins erhöht. Gilt für Nachrichten, die aufgrund ihrer Größe gefiltert werden, Nachrichten, die bei Anti-Relay- und Directory-Harvest-Prüfungen durchfallen, und Nachrichten, die beschädigten Inhalt, geschützten Inhalt, verschlüsselten Inhalt oder signierten Inhalt enthalten.

HINWEIS: Aufgrund der Weise, wie das Dashboard Zähler aggregiert, gibt es eine kleine Differenz zwischen den Informationen, die im Dashboard angezeigt werden, und denen, die in einem geplanten Bericht enthalten sind.

Information zu Statistiken, die in der Liste "E-Mail-Warteschlangen" angezeigt werden

Diese Informationen gelten für die Warteschlangen **In der Warteschlange**, **Isoliert** und **Anfragen für Entlassen aus Quarantäne**:

- Wenn eine Nachricht an zwei Empfänger gesendet und in die Zustellungswarteschlange gestellt wird (beispielsweise, weil der weiterführende MTA ausgefallen ist), gilt Folgendes:
  - Die Anzahl der Elemente in der Warteschlange ist 1, da die Appliance eine Nachricht empfangen hat.
  - Die Anzahl der Empfänger ist 2, da die Nachricht zwei Empfänger hat.

  HINWEIS: Wenn Sie auf den Link **In der Warteschlange** klicken, werden zwei Elemente angezeigt, da für jeden Empfänger eine Nachricht vorhanden ist.
- Wenn zwei Nachrichten an einen Empfänger gesendet und in die Zustellungswarteschlange gestellt werden (beispielsweise, weil der weiterführende MTA ausgefallen ist), gilt Folgendes:
  - Die Anzahl der Elemente in der Warteschlange ist 2, da die Appliance zwei Nachrichten empfangen hat.

- Die Anzahl der Empfänger ist 2, da jede Nachricht einen Empfänger hat.

HINWEIS: Wenn Sie auf den Link **In der Warteschlange** klicken, werden zwei Elemente angezeigt.

Vorgehensweise – Deaktivieren des Warnhinweises "McAfee Global Threat Intelligence-Feedback deaktiviert"

Die Appliance zeigt standardmäßig eine Warnmeldung an, wenn das McAfee Global Threat Intelligence-Feedback (GTI-Feedback) nicht aktiviert ist, da es von McAfee als bewährte Vorgehensweise angesehen wird, diese Form der Kommunikation zu aktivieren.

1. Wählen Sie im Appliance-Dashboard im Bereich "Systemstatus" die Option **Bearbeiten** aus.
2. Deaktivieren Sie **Einen Warnhinweis anzeigen, wenn McAfee GTI-Feedback nicht aktiviert ist**.
3. Klicken Sie auf **OK**.

Testen der Konfiguration der Virtual Appliance

Diese Informationen beschreiben, wie Sie testen können, ob die McAfee Email Security Virtual Appliancenach der Installation ordnungsgemäß funktioniert.

Inhalt

- Testen der Verbindung
- Aktualisieren der DAT-Dateien
- Testen von E-Mail-Verkehr und Virenerkennung
- Testen der Spam-Erkennung

Testen der Verbindung

Gehen Sie wie nachfolgend beschrieben vor, um die grundlegende Verbindungsfähigkeit zu bestätigen. Die McAfee Email Security Virtual Appliance prüft, ob sie mit dem Gateway, den Update-Servern und den DNS-Servern kommunizieren kann. Sie bestätigt außerdem, dass der Name der virtuellen Appliance und der Domänenname gültig sind.

Vorgehensweise

1. Öffnen Sie die Seite **Systemtests** mit einer der folgenden Methoden:
   - Wählen Sie im Bereich **Tasks** des Dashboards die Option **Systemtests ausführen**.
   - Wählen Sie in der Navigationsleiste die Option **Fehlerbehebung**.
2. Wählen Sie die Registerkarte **Tests**.
3. Klicken Sie auf **Tests starten**. Jeder Test sollte positiv beendet werden.

Aktualisieren der DAT-Dateien

Um sicherzugehen, dass die McAfee Email Security Virtual Appliance über die aktuellsten Erkennungsdefinitionsdateien (DAT) verfügt, empfehlen wir, diese zu aktualisieren, bevor Sie die Scanoption konfigurieren.

Im Rahmen der Verwendung der virtuellen Appliance können Sie einzelne Arten von Definitionsdateien aktualisieren sowie die standardmäßig geplanten Aktualisierungen an Ihre Anforderungen anpassen.

Vorgehensweise

1. Öffnen Sie die Seite **Aktualisierungen** mit einer der folgenden Methoden:
   - Wählen Sie im Bereich **Systemstatus** des Dashboards die Option **Aktualisierungen**.

- Wählen Sie **System | Komponentenverwaltung | Aktualisierungsstatus**.

2 Wenn Sie alle DAT-Dateien aktualisieren möchten, klicken Sie auf **Jetzt aktualisieren**.

3 Um zu gewährleisten, dass die virtuelle Appliance über den aktuellsten Software-Patch verfügt, gehen Sie zum Produkt-Dashboard, wählen Sie **Aktualisierungen**, und klicken Sie auf **Jetzt aktualisieren**.

Testen von E-Mail-Verkehr und Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um zu prüfen, ob E-Mail-Verkehr erfolgreich durch die McAfee Email Security Virtual Appliance geleitet wird und ob Bedrohungen ordnungsgemäß identifiziert werden. Wir verwenden die EICAR-Testdatei, eine harmlose Datei, die eine Virenerkennung auslöst.

Vorgehensweise

1 Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.

2 Sehen Sie sich im Dashboard den Bereich **E-Mail-Erkennungen** an. Aus der Liste für das Protokoll, das Sie zum Versenden der Nachricht verwendet haben, sollte hervorgehen, dass eine Nachricht empfangen wurde.

3 Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

4 Speichern Sie die Datei unter dem Namen EICAR.COM.

5 Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.

6 Kehren Sie zum Dashboard zurück, und sehen Sie sich den Bereich **E-Mail-Erkennungen** an. Sie sollten sehen, dass ein Virus erkannt wurde.

7 Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.

Testen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um einen "General Test mail for Unsolicited Bulk Email" (Allgemeinen Test auf unerwünschte Bulk-E-Mails – GTUBE) auszuführen, mit dem geprüft wird, ob eingehender Spam erkannt wird.

Vorgehensweise

1 Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.

2 Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
Achten Sie darauf, dass der Text keine Zeilenumbrüche enthält.

3 Senden Sie die neue E-Mail an eine interne Posteingangsadresse. Die Software scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.

Funktionen der Virtual Appliance

In diesem Abschnitt finden Sie Vorgehensweisen zur Demonstration der Scan-Funktionen von McAfee Email Security Virtual Appliance. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Inhalt

- Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk
- Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln
- Vermeiden des Verlusts vertraulicher Daten
- Bearbeiten von isolierten Nachrichten
- Überwachen der Spam-Erkennung
- Steuern des Benutzerzugriffs auf Basis einer Rolle

Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk

Eine Richtlinie ist eine Zusammenstellung von Einstellungen und Regeln, die der McAfee Email Security Virtual Appliance mitteilen, wie bestimmte Gefahren für Ihr Netzwerk abgewehrt werden sollen. Wenn Sie Echtzeitscan-Richtlinien für Ihr Unternehmen erstellen, müssen Sie Ihre Anforderungen in Ruhe analysieren und planen. Hinweise für die Richtlinienplanung finden Sie in der Online-Hilfe, die über die Produktbenutzeroberfläche aufgerufen werden kann.

Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln

Verwenden Sie Compliance-Scans zur Unterstützung der Compliance mit gesetzlichen und betrieblichen Auflagen. Sie können aus einer Bibliothek aus vordefinierten Compliance-Regeln wählen oder eigene Regeln und Wörterbücher für Ihr Unternehmen erstellen.

Compliance-Regeln können hinsichtlich ihrer Komplexität von einem einfachen Auslöser bei der Erkennung eines einzelnen Begriffs in einem Wörterbuch bis hin zum Aufbauen auf und Kombinieren von faktorbasierten Wörterbüchern variieren, die nur auslösen, wenn ein bestimmter Schwellenwert erreicht wird. Mithilfe der erweiterten Funktionen von Compliance-Regeln können Wörterbücher mit den logischen Operationen *eines von*, *alle von* oder *außer* kombiniert werden.

1 Gehen Sie wie folgt vor, um E-Mail-Nachrichten zu blockieren, die die Richtlinie "Bedrohliche Sprache" verletzen:

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

c Klicken Sie auf **Neue Regel aus Vorlage erstellen**, um den Assistenten für die Regelerstellung zu öffnen.

d Wählen Sie die Richtlinie **Zulässige Nutzung - Bedrohliche Sprache** aus, und klicken Sie auf **Weiter**.

e Sie können den Namen der Regel optional ändern. Klicken Sie anschließend auf **Weiter**.

f Ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.

g Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

2 Gehen Sie wie folgt vor, um eine einfache benutzerdefinierte Regel zum Blockieren von E-Mail-Nachrichten zu erstellen, die Sozialversicherungsnummern enthalten

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

c Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.

d Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

e Geben Sie im **Suchfeld** sozial ein.

f Wählen Sie das Wörterbuch **Sozialversicherungsnummer** aus, und klicken Sie zweimal auf **Weiter**.

g Wählen Sie die Aktion **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.

3 Gehen Sie wie folgt vor, um eine komplexe Regel zu erstellen, die auslöst, wenn sowohl Wörterbuch A als auch Wörterbuch B erkannt werden, jedoch nicht, wenn darüber hinaus auch Wörterbuch C erkannt wird.

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

c Klicken Sie auf **Neue Regel erstellen**, um den Assistenten für die Regelerstellung zu öffnen.

d Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

e Wählen Sie zwei Wörterbücher aus, die in die Regel aufgenommen werden sollen, und klicken Sie auf **Weiter**.

f Wählen Sie in der Ausschlussliste ein Wörterbuch aus, das Sie von der Regel ausschließen möchten.

g Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die Regel ausgelöst wird.

h Wählen Sie im Dropdown-Feld **Und bedingt** die Option **Alle** aus, und klicken Sie auf **Fertig stellen**.

4 Gehen Sie wie folgt vor, um ein neues Wörterbuch zu einer vorhandenen Regel hinzuzufügen:

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Erweitern Sie die Regel, die Sie bearbeiten möchten.

c Wählen Sie **Wörterbuch hinzufügen**.

d Wählen Sie das neue Wörterbuch aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

5 Gehen Sie wie folgt vor, um eine "Unzufriedenheit"-Regel zu konfigurieren, die mit einem niedrigen Schwellenwert überwacht wird und bei einem hohen Schwellenwert blockiert:

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Klicken Sie auf **Neue Regel erstellen**, geben Sie einen Namen für die Regel ein, beispielsweise Unzufriedenheit - Niedrig, und klicken Sie auf **Weiter**.

c Wählen Sie das Wörterbuch "Unzufriedenheit" aus, und geben Sie unter "Schwelle" den Wert 20 ein.

d Klicken Sie auf **Weiter** und anschließend erneut auf **Weiter**.

e Akzeptieren Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Standardaktion.

f Klicken Sie auf **Fertig stellen**.

g Wiederholen Sie die Schritte 2 bis 4, um eine weitere neue Regel zu erstellen. Nennen Sie diese jedoch Unzufriedenheit – Hoch, und weisen Sie ihr den Schwellenwert 40 zu.

h Wählen Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Option **Daten akzeptieren und anschließend verwerfen (Blockieren)** aus.

i Klicken Sie auf **Fertig stellen**.

j Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

6 Gehen Sie wie folgt vor, um den Schwellenwert zu bearbeiten, der einer vorhandenen Regel zugeordnet ist. Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch "Vergütung und Leistungen":

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Erweitern Sie die Regel, die Sie bearbeiten möchten, und wählen Sie anschließend das Symbol "Bearbeiten" neben dem Wörterbuch aus, dessen Faktor Sie ändern möchten.

c Geben Sie unter "Schwellenwert für Wörterbuch" den Faktor ein, bei dem die Regel ausgelöst werden soll, und klicken Sie auf **OK**.

7 Gehen Sie wie folgt vor, um den Faktorbeitrag eines Wörterbuchbegriffs zu beschränken. Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch "Vergütung und Leistungen". Bei solchen Wörterbüchern können Sie beschränken, wie oft ein Begriff zum Gesamtfaktor beitragen kann.

a Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

b Erweitern Sie die Regel, die Sie bearbeiten möchten, und klicken Sie anschließend auf das Symbol "Bearbeiten" neben dem Wörterbuch, dessen Faktor Sie ändern möchten.

c Geben Sie unter **Max. Begriffsanzahl** die maximale Anzahl an Vorkommnissen eines Begriffs an, die zum Gesamtfaktor beitragen sollen.

Vermeiden des Verlusts vertraulicher Daten

Gehen Sie wie nachfolgend beschrieben vor, um das Versenden eines vertraulichen Finanzdokuments aus Ihrem Unternehmen heraus zu blockieren.

Vorgehensweise

1. Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Registrierte Dokumente**, erstellen Sie die Kategorie Finanzen, und laden Sie Dokumente in diese Kategorie hoch.
2. Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinie**, und wählen Sie die **Data Loss Prevention**-Richtlinie aus.
3. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
4. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste "Regeln" angezeigt wird.
5. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **OK**.
6. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Bearbeiten von isolierten Nachrichten

Gehen Sie wie nachfolgend beschrieben vor, um nach E-Mails zu suchen, die aufgrund von Compliance-Problemen isoliert wurden, und geben Sie die Nachricht an den vorgesehenen Empfänger frei.

Vorgehensweise

1. Klicken Sie auf **E-Mail | Nachrichtensuche**.
2. Wählen Sie **Isoliert** in der Dropdown-Liste **Nachrichtenstatus** aus.
3. Klicken Sie auf **Suchen/Aktualisieren**.

   Alle isolierten Nachrichten werden im unteren Bereich der Seite angezeigt.
4. Um die E-Mails zu finden, die aufgrund von Compliance-Problemen in Quarantäne verschoben wurden, wählen Sie **Compliance** in der Dropdown-Liste **Kategorie** aus.
5. Klicken Sie auf **Suchen/Aktualisieren**.

   Der untere Bereich des Bildschirms wird aktualisiert, um nur die Nachrichten anzuzeigen, die aufgrund von Compliance-Problemen isoliert wurden.
6. Um eine E-Mail anzuzeigen, die aufgrund von Compliance-Problemen in Quarantäne verschoben wurde, wählen Sie die entsprechende isolierte Nachricht mit Hilfe des Kontrollkästchens links auf der Seite aus.
7. Klicken Sie auf **Nachricht anzeigen**.

   Die ausgewählte Nachricht wird in einem neuen Fenster angezeigt. In diesem Fenster können Sie den Inhalt der E-Mail lesen. Außerdem können Sie alternativ die detaillierten Informationen des E-Mail-Headers anzeigen.
8. Klicken Sie auf **Ausgewählte Elemente aus Quarantäne entlassen**, um die isolierte E-Mail freizugeben.

Die ausgewählte E-Mail wird aus der Quarantäne entlassen.

HINWEIS: E-Mails mit infiziertem Inhalt können nicht aus der Quarantäne entlassen werden, da dies Schäden auf Ihren Systemen verursachen könnte.

Überwachen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um die Spam-Erkennungsrate mit der standardmäßigen SMTP-Spam-Erkennungsrichtlinie überwachen. Sobald Sie die Konfigurationskonsole ausgeführt haben, funktionieren diese Einstellungen und schützen Ihr Netzwerk und Ihre Benutzer vor unerwünschten Spam-Nachrichten. Eine ausführlichere Erläuterung der Einstellungen finden Sie in der Online-Hilfe, die über die Benutzeroberfläche aufgerufen werden kann.

Standardmäßig führt die Email Security Virtual Appliance folgende Aufgaben aus:

- Sie blockiert Phishing-Nachrichten.
- Sie markiert Nachrichten mit einer Einstufung von mindestens fünf als Spam.
- Sie verwirft Spam-Nachrichten mit einer Einstufung von mindestens zehn.
- Die Absenderauthentifizierung ist aktiviert.

Mithilfe dieser Standardeinstellungen erkennt die virtuelle Appliance mehr als 98 % aller Spam-Nachrichten.

HINWEIS: Die Einstellungen für die Absenderauthentifizierung umfassen die E-Mail-Reputation von McAfee Global Threat Intelligence. Wenn ein Absender die E-Mail-Reputation-Prüfung von McAfee Global Threat Intelligence nicht besteht, weist die virtuelle Appliance die E-Mail zurück, beendet die Verbindung und lässt die IP-Adresse des Absenders nicht mehr zu. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und automatisch zehn Minuten lang auf Kernel-Ebene blockiert (die standardmäßige Blockierdauer kann geändert werden). Im Bereich **E-Mail-Erkennungen** des Dashboards wird die Anzahl der blockierten Verbindungen angezeigt.

Vorgehensweise

1. Wählen Sie im Bereich **Scan-Richtlinien** des Dashboards die Option **SMTP | Standardrichtlinie**, um die Standardeinstellungen für die Spam-Erkennung anzuzeigen.
2. Vergewissern Sie sich, dass Spam-Nachrichten ordnungsgemäß identifiziert werden, indem Sie eine Nachricht die virtuelle Appliance passieren lassen, bei der die Einstellungen zur Spam-Erkennung aktiviert werden.
3. Wenn Sie die Erkennungsrate überwachen möchten, kehren Sie zum Dashboard zurück, und betrachten Sie den Bereich **E-Mail-Erkennungen**.
   Die Zahl für **Spam und Phishing** und für **Absenderauthentifizierung** wird hochgezählt. Die Zahl für die Absenderauthentifizierungserkennungen beinhaltet die Anzahl der Absender, die die E-Mail-Reputation-Prüfung von McAfee Global Threat Intelligence nicht bestanden haben. **E-Mail-Diagramme** bietet eine graphische Darstellung der Daten.
4. Wenn Sie einen Bericht über die E-Mail-Aktivität erhalten möchten, gehen Sie zu **Tasks**, und wählen Sie **Bevorzugte E-Mail-Berichte anzeigen**.
5. Sehen Sie sich den Bericht **Blockiert (heute)** und den Bericht **Häufigste Spam-Absender (heute)** an.

Steuern des Benutzerzugriffs auf Basis einer Rolle

Gehen Sie wie nachfolgend beschrieben vor, um einen Benutzer zu erstellen, der nur Berichte zu den Aktivitäten der McAfee Email Security Virtual Appliance erstellen und anzeigen kann.

Vorgehensweise

1. Wählen Sie im Dashboard im Bereich **Tasks** die Option **Benutzer verwalten**.
2. Wählen Sie unter **Benutzerkonten und Regeln** die Option **Benutzer hinzufügen**.
3. Geben Sie einen Benutzernamen ein, beispielsweise exampleuser. Wählen Sie unter **Rolle** die Option **Berichtadministrator**.
4. Geben Sie ein Kennwort ein, wiederholen Sie die Eingabe zur Bestätigung, klicken Sie auf **OK**, und übernehmen Sie die Änderungen. Der neue Benutzer wird in der Liste mit den **Konten** mit der Rolle **Berichtadministrator** aufgeführt.
5. Melden Sie sich ab und dann wieder an, und zwar mit den Anmeldeinformationen des soeben erstellten Benutzers.
6. Auf der Benutzeroberfläche ist Folgendes zu sehen:
   - Die Navigationsleiste enthält nur die Symbole für **Dashboard** und **Berichte**.
   - Sämtliche Statusinformationen werden angezeigt, können jedoch nicht bearbeitet werden.
   - Die Liste **Tasks** enthält lediglich berichtsbezogene Optionen, etwa **Geplante Berichte verwalten**.

Zusätzliche Konfigurationsoptionen

Diese Informationen geben Ihnen einige Tipps zu bewährten Vorgehensweisen und stellen Ihnen einige erweiterte Konfigurationsoptionen vor.

Inhalt

- Aktualisieren auf Email Security Virtual Appliance 5.6
- Installieren der virtuellen Appliance auf VMware Server 2.0 unter Microsoft Windows
- Installieren der virtuellen Appliance auf VMware Server 1.0 unter Microsoft Windows
- Ausführen einer virtuellen Appliance auf VMware Server im Betriebsmodus "Transparent"
- Ausführen einer virtuellen Appliance VMware ESX, VMware vSphere oder VMware ESXi in einem transparenten Betriebsmodus
- Ändern der standardmäßigen Aktionen zum Ausschalten und Zurücksetzen
- Konfigurieren der Optionen zum Herunterfahren und Neustart
- Konvertieren von einer VMtrial-Installation

Aktualisieren auf Email Security Virtual Appliance 5.6

Gehen Sie wie nachfolgend beschrieben vor, um ein Upgrade auf McAfee Email Security Virtual Appliance 5.6 mithilfe des ISO-Images der Software durchzuführen.

HINWEIS: Email and Web Security Virtual Appliance 5.5 oder Email and Web Security Virtual Appliance 5.6 müssen bereits installiert sein.

Vorgehensweise

HINWEIS: Nachdem ein Betriebssystem auf einer virtuellen Appliance installiert wurde, startet die virtuelle Maschine immer zuerst direkt von der Festplatte. Um diese Funktion zu umgehen, müssen Sie die virtuelle Maschine herunterfahren und eine Startverzögerung beim Hochfahren konfigurieren, so dass Sie genügend Zeit haben, auf das **Boot**-Menü zuzugreifen und stattdessen das Starten über die Installations-CD zu veranlassen.

1. Laden Sie die ZIP-Datei von Email Security Virtual Appliance 5.6 von der McAfee-Download-Website herunter, und extrahieren Sie sie.
2. Fahren Sie die virtuelle Appliance herunter:
   a. Melden Sie sich bei der Benutzeroberfläche der virtuellen Appliance an, und gehen Sie auf **System | Systemadministration | Systembefehle**.
   b. Geben Sie das Kennwort ein.
   c. Wählen Sie **Appliance beenden**.

3 Melden Sie sich beim VMware ESX-Server an, oder verwenden Sie den VMware Infrastructure Client oder den VMware vSphere Client, um sich beim VMware Virtual Center Server anzumelden.

4 Aktivieren Sie eine **Power-on-Boot**-Verzögerung, damit Sie ausreichend Zeit haben, die virtuelle Maschine von der CD aus starten zu lassen:

   a Wählen Sie die virtuelle Appliance in Liste **Inventory** (Inventar), und klicken Sie auf **Summary** (Zusammenfassung).

   b Wählen Sie **Edit Settings | Options | Boot Options** (Einstellungen bearbeiten | Optionen | Boot-Optionen).

   c Geben Sie unter **Power-on-Boot Delay** (Power-on-Boot-Verzögerung) 10,000 in das Textfeld ein, und klicken Sie auf **OK**.

5 Schalten Sie die virtuelle Appliance ein.

6 Stellen Sie sicher, dass sich der Mauszeiger in der Virtual Appliance-Konsole befindet. Drücken Sie anschließend die ESC-Taste, um das **Boot Menu** (Boot-Menü) zu öffnen.

   VORSICHT: Wählen Sie noch keine Optionen.

7 Ziehen Sie den Mauszeiger aus der Konsole, und wählen Sie **Connect CD/DVD 1** (CD/DVD1 verbinden).

8 Gehen Sie zu dem Ordner, in den Sie die Zip-Datei von Email Security Virtual Appliance 5.6 extrahiert haben, und doppelklicken Sie auf **<McAfee-EWS-SMG-5.6-<Build-Nummer>.Vmbuy.iso>**.

9 Wenn die ISO-Datei verbunden ist, klicken Sie erneut auf das Konsolenfenster. Wählen Sie **CD-ROM Drive** (CD-ROM-Laufwerk) aus, und drücken Sie die EINGABE-Taste.

10 Die virtuelle Appliance startet von der ISO-Datei.

11 Geben Sie **j** ein, um den Bedingungen der Endbenutzer-Lizenzvereinbarung zuzustimmen.

12 Wählen Sie die gewünschte Upgrade-Option, und drücken Sie die Eingabetaste, um das Upgrade durchzuführen.

13 Geben Sie **j** ein, um zu bestätigen, dass Sie fortfahren möchten.

Installieren der virtuellen Appliance auf VMware Server 2.0 unter Microsoft Windows

Gehen Sie wie nachfolgend beschrieben vor, um McAfee Email Security Virtual Appliance auf einem Host-Computer zu installieren, auf dem VMware Server 2.0 ausgeführt wird.

HINWEIS: Um optimale Leistung und Durchsatz in einer virtuellen Umgebung zu erzielen, empfiehlt McAfee, dass Sie die virtuelle Appliance auf VMware vSphere ausführen. Siehe Installieren der virtuellen Appliance auf VMware ESX oder VMware ESXi oder Installieren der virtuellen Appliance auf VMware vSphere und VMware vSphere Hypervisor (ESXi).

VMware Server 2.0 erfordert die Installation von Java Runtime Environment (JRE) auf dem Host-Computer. Wenn JRE nicht bereits installiert ist, erledigt dies VMware Server 2.0 für Sie.

HINWEIS: VMware Server 2.0 ist für die Ausführung der Virtual Appliance in einer Testumgebung oder in kleineren Installationen geeignet. Nach der Installation von VMware Server 2.0 empfiehlt McAfee, dass Sie DHCP im virtuellen VMnet0-Netzwerk deaktivieren, um einen Konflikt mit DHCP-Diensten zu vermeiden, die in Ihrem physischen Netzwerk ausgeführt werden.

Wenn Sie das Produkt Email Security Appliance (VMtrial) verwendet haben, um die Software zu testen, können Sie Ihre VMtrial-Konfiguration speichern und auf der virtuellen Appliance wiederherstellen, wenn die Installation abgeschlossen ist.

Vorbereitung

- Laden Sie die ZIP-Datei des Pakets, das die Installationsdateien für VMware ESX und VMware Server enthält, von der McAfee-Download-Seite herunter, und extrahieren Sie sie auf dem Host-Computer.
- Laden Sie VMware Server 2.0 herunter, und notieren Sie Ihre Registrierungs-ID.
- Wenn Sie VMware Server 2.0 unter Microsoft Windows ausführen, empfiehlt McAfee, dass Sie die Windows-Update-Funktion auf **Updates downloaden, aber Installationszeitpunkt manuell festlegen** einstellen, um zu verhindern, dass das Betriebssystem neu startet, nachdem die Updates installiert wurden, und die virtuellen Festplatten dadurch beschädigt werden.

Vorgehensweise

1. Öffnen Sie die VMware Server Infrastructure Web Access-Konsole (**Start | VMware | VMware Server Home Page (VMware Server-Homepage)**).
2. Melden Sie sich mit Ihrem Microsoft Windows-Anmeldenamen und -Kennwort an.
3. Klicken Sie in **Commands** (Befehle) auf **Add Datastore** (Datenspeicher hinzufügen), und geben Sie einen Namen dafür ein. Geben Sie den gesamten Verzeichnispfad, in den Sie zuvor die VMX-Datei extrahiert haben, ein, und klicken Sie auf **OK.**
4. Halten Sie den VMware Server-DHCP-Server an, um eine Störung des DHCP-Servers in Ihrem Netzwerk zu vermeiden.
   a. Öffnen Sie den Virtual Network Editor (**Start | VMware | VMware Server | Manage Virtual Networks** (Virtuelle Netzwerke verwalten)). Wenn Sie das Betriebssystem Microsoft Windows Vista verwenden, klicken Sie mit der rechten Maustaste auf **Manage Virtual Networks** (Virtuelle Netzwerke verwalten), und wählen Sie **Run as administrator** (Als Administrator ausführen).
   b. Klicken Sie auf die Registerkarte **DHCP**.
   c. Klicken Sie auf **Stop** (Anhalten) und anschließend auf **OK**.
5. Fügen Sie Email Security Virtual Appliance als virtuelle Maschine hinzu:
   a. Gehen Sie unter VMware Infrastructure Web Access auf den Bereich **Commands** (Befehle), wählen Sie **Add Virtual Machine to Inventory** (Virtuelle Maschine zum Inventar hinzufügen) aus, und wählen Sie den Datenspeicher aus, den Sie zuvor erstellt haben.
   b. Wählen Sie die VMX-Datei von McAfee in der Liste **Contents** (Inhalt), und klicken Sie auf **OK**. Anschließend sollte die Datei in der Liste **Inventory** (Inventar) zu sehen sein.
6. Stellen Sie die Hardware-Optionen so ein, dass die virtuelle Appliance entweder auf Ihrem Netzwerk ausgeführt wird, um den Datenverkehr zu scannen, oder auf dem Host-Computer.

   HINWEIS: Um Netzwerk-Loops zu vermeiden, empfiehlt McAfee, bei Ausführung des VMware Server im Modus "Nur Host" die virtuelle Appliance *nicht* im Modus "Transparente Bridge" zu betreiben.

   a. Wählen Sie in der VMware Infrastructure Web Access-Konsole die virtuelle Maschine aus.
   b. Wählen Sie in der Liste **Hardware** (Hardware) **Network Adapter 1** (Netzwerkadapter 1), und klicken Sie auf **Edit** (Bearbeiten). Ändern Sie die

Hardware-Optionen Ihren Anforderungen entsprechend. Wiederholen Sie den Vorgang für Network Adapter 2 (Netzwerkadapter 2).

c Klicken Sie auf **OK**.

7 Wählen Sie unter VMware Infrastructure Web Access die virtuelle Maschine der Email Security Virtual Appliance aus, und klicken Sie auf die grüne Schaltfläche, um sie zu starten.

8 Ansicht der Konsole der virtuellen Maschine:

a Wählen Sie unter VMware Infrastructure Web Access die Option **Console** (Konsole), und klicken Sie auf eine beliebige Stelle in dem schwarzen Fenster. Eventuell werden Sie gebeten, bei der ersten Installation das Konsolen-Plug-in für den VMware Remote Access (Remote-Zugriff) zu installieren.

b Akzeptieren Sie die Lizenzvereinbarung.

c Wählen Sie **1**.

d Geben Sie **j** ein, um zu bestätigen, dass Sie fortfahren möchten, und warten Sie, bis die virtuelle Appliance installiert ist. Das Eröffnungsfenster der Email Security Virtual Appliance wird angezeigt.

9 Wählen Sie im Eröffnungsfenster die Sprache aus, die Sie verwenden möchten.

10 Stimmen Sie den Bedingungen des Lizenzvertrags zu.

11 Führen Sie die Konfiguration mithilfe des grafischen Konfigurationsassistenten durch.

HINWEIS: Wenn Sie mit den Einstellungen im grafischen Konfigurationsassistenten nicht vertraut sind, verwenden Sie den Fensterbereich "Schnellhilfe" links im Inhaltsbereich. Wenn Sie die Schnellhilfe in einem neuen Fenster anzeigen möchten, klicken Sie auf das Hilfesymbol in der Navigationsleiste.

12 Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, und warten Sie, bis die Einstellungen übernommen wurden.

13 So melden Sie sich an:

a Geben Sie in einem Browser in demselben Netzwerk wie die Appliance https://<IP-Adresse> ein.

b Akzeptieren Sie die Sicherheitszertifikate.

c Geben Sie im Anmeldefenster den **Benutzernamen** scmadmin und das Kennwort ein.

Installieren der virtuellen Appliance auf VMware Server 1.0 unter Microsoft Windows

Gehen Sie wie nachfolgend beschrieben vor, um McAfee Email Security Virtual Appliance auf einem Host-Computer zu installieren, auf dem VMware Server 1.0 ausgeführt wird.

HINWEIS: Um optimale Leistung und Durchsatz in einer virtuellen Umgebung zu erzielen, empfiehlt McAfee, dass Sie die virtuelle Appliance auf VMware ESX Server 3.5 oder VMware ESXi ausführen. Siehe Installieren der virtuellen Appliance auf VMware ESX oder VMware ESXi oder Installieren der virtuellen Appliance auf VMware vSphere und VMware vSphere Hypervisor (ESXi).

HINWEIS: VMware Server ist für die Ausführung der virtuellen Appliance in einer Testumgebung oder in kleineren Installationen geeignet. Nach der Installation von VMware Server empfiehlt

McAfee, dass Sie DHCP im virtuellen VMnet0-Netzwerk deaktivieren, um einen Konflikt mit DHCP-Diensten zu vermeiden, die in Ihrem physischen Netzwerk ausgeführt werden.

Wenn Sie das Produkt Email Security Appliance (VMtrial) verwendet haben, um die Software zu testen, können Sie Ihre VMtrial-Konfiguration speichern und auf der virtuellen Appliance wiederherstellen, wenn die Installation abgeschlossen ist.

Vorbereitung

- Laden Sie die ZIP-Datei des Pakets, das die Installationsdateien für VMware ESX und VMware Server enthält, von der McAfee-Download-Seite herunter, und extrahieren Sie sie auf dem Host-Computer.
- Laden Sie VMware Server herunter, und notieren Sie Ihre Registrierungs-ID.
- Wenn Sie VMware Server unter Microsoft Windows ausführen, empfiehlt McAfee, dass Sie die Windows-Update-Funktion auf **Updates downloaden, aber Installationszeitpunkt manuell festlegen** einstellen, um zu verhindern, dass das Betriebssystem neu startet, nachdem die Updates installiert wurden, und die virtuellen Festplatten dadurch beschädigt werden.

Vorgehensweise

1. Gehen Sie auf dem Hostcomputer *zu dem Speicherort, an den Sie die Inhalte der ZIP-Datei für die virtuelle Appliance extrahiert haben.*

   HINWEIS: Vergewissern Sie sich, dass dies der Speicherort ist, an dem Sie die virtuelle Appliance ausführen möchten. Anderenfalls verschieben Sie die Datei, bevor Sie mit der Installation fortfahren.

2. Öffnen Sie den Ordner **McAfee-EWS-SMG-5.6....**, der die Installationsdateien für die Email Security Virtual Appliance enthält.
3. Doppelklicken Sie auf die Konfigurationsdatei **EWS-SMG-5.6<Paket-Nummer>.VMX**.

   Die VMware Server-Konsole wird gestartet und listet die neue virtuelle Maschine in der Inventarliste auf.

4. Klicken Sie in der Liste **Inventory** (Inventar) mit der rechten Maustaste auf das Element MWS, und wählen Sie **Settings** (Einstellungen).
5. Überprüfen Sie, dass **Ethernet** auf den **Bridged**-Modus (Bridge-Modus) eingestellt ist und dass **Ethernet2** auf den Modus **Host-only** (Nur Host) eingestellt ist.
6. Wählen Sie unter der Ansicht **Summary** (Zusammenfassung) der VMware Server-Konsole **Start this virtual machine** (Diese virtuelle Maschine starten) aus. Das Fenster auf der rechten Seite zeigt die Startup-Sequenz der virtuellen Appliance.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung.
8. Wählen Sie **1**, um eine vollständige Installation auszuführen, und wählen Sie dann **j**, um Ihre Auswahl zu bestätigen. Warten Sie, während Email Security Virtual Appliance installiert wird. Der grafische Konfigurationsassistent wird angezeigt.
9. Konfigurieren Sie die Einstellungen mithilfe des grafischen Konfigurationsassistenten der Email Security Virtual Appliance.

   HINWEIS: McAfee empfiehlt, dass Sie die virtuelle Appliance im standardmäßigen Modus "Expliziter Proxy" betreiben. Auf einem standardmäßigen VMware Server sind drei virtuelle Netzwerke zur Verwendung mit der virtuellen Appliance verfügbar, die unverändert belassen werden können, wenn Sie die virtuelle Appliance im Modus "Expliziter Proxy" betreiben:

- VMnet0 (Bridge) – Es wird automatisch eine Bridge zwischen dem Netzwerk und einem der physischen Netzwerkadapter Ihres Host verwendet.
- VMnet1 (Nur Host) – Es wird ein privates Netzwerk für den Host freigegeben. Es besteht keine Bridge zwischen diesem Netzwerk und den physischen Netzwerkadaptern des Hosts.
- VMnet8 (NAT) – Ein weiteres privates Netzwerk wird für den Host freigegeben. Es verwendet die Network Address Translation (Netzwerkadressübersetzung), um die IP-Adresse des Hosts freizugeben.

HINWEIS: Wenn Sie mit den Einstellungen im grafischen Konfigurationsassistenten nicht vertraut sind, verwenden Sie den Fensterbereich "Schnellhilfe" links im Inhaltsbereich. Wenn Sie die Schnellhilfe in einem neuen Fenster anzeigen möchten, klicken Sie auf das Hilfesymbol in der Navigationsleiste.

10 Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, und warten Sie, bis die Einstellungen übernommen wurden.

11 So melden Sie sich an:

a Geben Sie in einem Browser in demselben Netzwerk wie die Appliance https://<IP-Adresse> ein.

b Akzeptieren Sie die Sicherheitszertifikate.

c Geben Sie im Anmeldefenster den **Benutzernamen** scmadmin und das Kennwort ein.

Ausführen einer virtuellen Appliance auf VMware Server im Betriebsmodus "Transparent"

Mithilfe dieses Tasks können Sie eine virtuelle Appliance so einstellen, dass sie in einem der transparenten Betriebsmodi betrieben wird.

Standardmäßig erstellt VMware Server nur eine Bridge-Schnittstelle. Um einen der transparenten Modi auf VMware Server auszuführen, benötigen Sie zwei Bridge-Schnittstellen.

HINWEIS: McAfee empfiehlt, dass Sie die McAfee Email Security Virtual Appliance im standardmäßigen Modus "Expliziter Proxy" betreiben und sie nicht so konfigurieren, dass sie in einem der transparenten Modi betrieben wird.

Vorbereitungen

Um die virtuelle Appliance entweder im Modus "Transparenter Router" oder im Modus "Transparente Bridge" zu betreiben, vergewissern Sie sich, dass Ihr Hostcomputer über zwei Netzwerkkarten verfügt.

Vorgehensweise

1 Verbinden Sie die Netzwerkschnittstellenkarten (Network Interface Cards, NIC) der virtuellen Appliance über ein virtuelles Netzwerk im Bridge-Modus mit der physischen Netzwerkschnittstelle des Host-Computers, um die zweite Bridge-Schnittstelle zu erstellen:

- Öffnen Sie unter VMware Server 1.0, das auf dem Betriebssystem Microsoft Windows ausgeführt wird, die VMware Server-Konsole, und wählen Sie **Host | Virtual Network Settings** (Virtuelle Netzwerkeinstellungen).
- Öffnen Sie unter VMware Server 2.0 den Virtual Network Editor (**Start | VMware | VMware Server | Manage Virtual Networks** (Virtuelle Netzwerke verwalten)).

Wenn Sie das Betriebssystem Microsoft Windows Vista verwenden, klicken Sie mit der rechten Maustaste auf **Manage Virtual Networks** (Virtuelle Netzwerke verwalten), und wählen Sie **Run as administrator** (Als Administrator ausführen).

- Öffnen Sie unter Linux eine Shell, und führen Sie das Skript vmware-config.pl aus. Befolgen Sie dann die Anweisungen zum **Networking Setup** (Netzwerk-Setup). Bestätigen Sie, dass Sie eine zweite Bridge-Schnittstelle erstellen möchten.

2 Wählen Sie **VM | Settings** (VM | Einstellungen), um die Schnittstellen der virtuellen Appliance mit den zwei Bridge-Schnittstellen zu verbinden.

3 Starten Sie die Email Security Virtual Appliance, und führen Sie den grafischen Konfigurationsassistenten aus.

4 Konfigurieren Sie die Appliance nach Bedarf als transparente Bridge oder transparenten Router.

Ausführen einer virtuellen Appliance VMware ESX, VMware vSphere oder VMware ESXi in einem transparenten Betriebsmodus

Gehen Sie wie nachfolgend beschrieben vor, um eine virtuelle Appliance einzurichten, die auf VMware ESX Server, VMware vSphere oder VMware ESXi ausgeführt wird und in einem der transparenten Betriebsmodi betrieben wird.

HINWEIS: McAfee empfiehlt, dass Sie die McAfee Email Security Virtual Appliance im standardmäßigen Modus "Expliziter Proxy" betreiben und sie nicht so konfigurieren, dass sie in einem der transparenten Modi betrieben wird.

Vorgehensweise

1 Erstellen Sie zwei virtuelle Switches für die beiden Netzwerkschnittstellen im physischen Netzwerk.

HINWEIS: Vergewissern Sie sich, dass jeder virtuelle Switch mit einer anderen physischen Netzwerk-Schnittstelle auf dem VMware-Host verbunden ist.

2 Folgen Sie den vorhergehenden Anweisungen aus diesem Handbuch, um die virtuelle Appliance auf dem virtuellen Host zu installieren, bis Sie die virtuelle Appliance mithilfe von OVF importieren müssen.

3 Um die virtuelle Appliance an das virtuelle Netzwerk anzuschließen, wählen Sie die beiden virtuellen Switches aus, die Sie in Schritt 1 erstellt haben.

Ändern der standardmäßigen Aktionen zum Ausschalten und Zurücksetzen

Gehen Sie wie nachfolgend beschrieben vor, um die Aktionen zum **Ausschalten** und **Zurücksetzen** im VMware ESX Server, VMware vSphere oder VMware ESXi so zu ändern, dass die McAfee Email Security Virtual Appliance heruntergefahren werden kann, ohne dass das Dateisystem der virtuellen Maschine beschädigt wird.

Vorgehensweise

1. Klicken Sie im **VMware Infrastructure Client** mit der rechten Maustaste auf die Email Security Virtual Appliance, und wählen Sie **Edit Settings** (Einstellungen bearbeiten) aus.
2. Gehen Sie zur Registerkarte **Options** (Optionen), und wählen Sie **VMware Tools** (VMware-Tools).
3. Setzen Sie die Option neben dem roten Kästchen auf **Shut Down Guest** (Gast herunterfahren).
4. Setzen Sie die Option neben dem Symbol **Reset** (Zurücksetzen) (roter und grüner Pfeil) auf **Restart Guest** (Gast neu starten).

Konfigurieren der Optionen zum Herunterfahren und Neustart

Gehen Sie wie nachfolgend beschrieben vor, um die McAfee Email Security Virtual Appliance so zu konfigurieren, dass sie automatisch heruntergefahren und neu gestartet wird, wenn Sie den VMware ESX-Server, VMware vSphere oder VMware ESXi neu starten.

Vorgehensweise

1. Wählen Sie den ESX Host aus, und klicken Sie auf die Registerkarte **Configuration** (Konfiguration).
2. Wählen Sie **Virtual Machine Startup/Shutdown** (Start/Herunterfahren der virtuellen Maschine) im Feld **Software** aus, klicken Sie auf **Properties** (Eigenschaften), und führen Sie folgende Schritte aus:
   - Aktivieren Sie die Option **Allow virtual machines to start and stop automatically with the system** (Virtuellen Maschinen das automatische Starten und Anhalten mit dem System erlauben).
   - Ändern Sie die **Shutdown Action** (Aktion bei Herunterfahren) in **Guest Shutdown** (Gast herunterfahren).
3. Wählen Sie Email Security Virtual Appliance aus der Liste, und klicken Sie auf **Move up** (Nach oben), bis es an oberster Stelle in der Liste erscheint.
4. Klicken Sie auf **Edit** (Bearbeiten).
5. Wählen Sie unter **Virtual Machine Autostart Settings** (Autostart-Einstellungen für die virtuelle Maschine) im Feld **Shutdown Settings** (Einstellungen für Herunterfahren) die Option **Use specified settings** (Angegebene Einstellungen verwenden) aus, und wählen Sie dann **Guest Shutdown** (Gast herunterfahren) neben **Perform shutdown action** (Aktion zum Herunterfahren durchführen).
6. Klicken Sie zwei Mal auf **OK**, um das Konfigurationsfenster zu schließen.

   Die virtuelle Appliance sollte nun in der Liste unter der Überschrift **Automatic Startup** (Automatischer Start) angezeigt werden, und der Wert in der Spalte **Shutdown** (Herunterfahren) sollte **Shut down guest** (Gast herunterfahren) lauten.

Konvertieren von einer VMtrial-Installation

Gehen Sie wie nachfolgend beschrieben vor, um beliebige Konfigurationseinstellungen von einer McAfee Email Security Appliance (VMtrial)-Installation auf die McAfee Email Security Virtual Appliance zu migrieren.

Vorgehensweise

1. Navigieren Sie in Ihrer VMtrial-Installation zu **System | Cluster-Verwaltung | Konfiguration sichern und wiederherstellen**.
2. Klicken Sie auf **Konfiguration sichern**, um die Konfigurationsdetails zu speichern.
3. Installieren Sie die Email Security Virtual Appliance-Software in der von Ihnen gewählten virtuellen Umgebung.
4. Melden Sie sich an, und öffnen Sie die Email Security Virtual Appliance-Software.
5. Navigieren Sie zu **System | Cluster-Verwaltung | Konfiguration sichern und wiederherstellen**, und klicken Sie auf **Aus Datei wiederherstellen**.
6. Blättern Sie zur VMtrial-Konfigurationsdatei, die Sie wiederherstellen möchten, und klicken Sie auf **Öffnen**.
7. Wählen Sie die Teile der Datei aus, die Sie wiederherstellen möchten, und klicken Sie auf **OK**.
8. Überprüfen Sie, ob die Einstellungen erfolgreich importiert wurden, und übernehmen Sie die Änderungen.

   HINWEIS: Weitere Informationen über das Sichern und Wiederherstellen der Konfiguration finden Sie im *Migrationshandbuch zur Email and Web Security Appliance*.

Fehlerbehebung bei der Virtual Appliance

In diesen Informationen sind Lösungen zu Problemen enthalten, die beim Installieren und Ausführen der McAfee Email Security Virtual Appliance auftreten können.

HINWEIS: Setzen Sie sich mit VMware in Verbindung, um Informationen zu Ihrem VMware-Produkt zu erhalten, oder besuchen Sie die VMware-Website http://www.vmware.com.

Inhalt

- Die Appliance empfängt keinen Datenverkehr aus dem Netzwerk
- Probleme mit der Benutzeroberfläche
- E-Mail-Probleme
- POP3
- Probleme bei der physischen Konfiguration
- Probleme bei der automatischen Aktualisierung der Antiviren-Software
- Probleme mit Anti-Spam

Die Appliance empfängt keinen Datenverkehr aus dem Netzwerk

Überprüfen Sie Folgendes:

- Die Appliance ist eingeschaltet und die Software wird ausgeführt.

  Wenn die LED des Netzschalters orange leuchtet, ist die Appliance angeschlossen, aber nicht eingeschaltet. Bei eingeschalteter Appliance leuchtet die LED des Netzschalters grün.
- Die Netzwerkkabel sind unbeschädigt und ordnungsgemäß an die Anschlüsse der Appliance und die vorhandenen Netzwerkkomponenten angeschlossen. Falls Sie nicht die im Lieferumfang der Appliance enthaltenen Kabel verwendet haben, stellen Sie sicher, dass Ihre Kabel der richtigen Spezifikation entsprechen.
- Ihre Netzwerkgeräte sind an die korrekten LAN-Anschlüsse der Appliance angeschlossen.
- Die Geschwindigkeiten der Netzwerkkarte und die Einstellungen für Voll- oder Halb-Duplex auf beiden Seiten der Verbindungen sind kompatibel, und die Einstellungen wurden korrekt automatisch ausgehandelt.
- Die LAN-LEDs leuchten.

Falls die Appliance immer noch keinen Netzwerkverkehr empfängt, überprüfen Sie die Netzwerkkabel und die Netzwerkanschlüsse an Ihren Netzwerkgeräten. Funktionieren Kabel und Anschlüsse ordnungsgemäß, liegt das Problem bei der Appliance. Wenden Sie sich an den Händler.

Probleme mit der Benutzeroberfläche

Dieser Abschnitt beinhaltet Lösungen zu Problemen, die beim Konfigurieren der Appliance über die Benutzeroberfläche auftreten können.

Warum gelange ich mit der Browser-Schaltfläche "Zurück" wieder zum Anmeldefenster?

Dies ist ein bekanntes Problem, das bei Verwendung der Webbrowser-Version der Appliance-Software auftritt. Verwenden Sie stattdessen die Appliance-Anwendung.

Ich kann nicht auf das Anmeldefenster zugreifen.

Überprüfen Sie Folgendes:

- Die Appliance ist eingeschaltet, und die Software wird ausgeführt. Das wird durch die leuchtende LED des Netzschalters und die nicht leuchtenden LEDs der Festplattenlaufwerke angezeigt.
- Sie haben im Adressfeld Ihres Webbrowsers **https** (und nicht **http**) verwendet. Stellen Sie sicher, dass Ihr Browser SSL-Verschlüsselung (SSL – Secure Sockets Layer) unterstützt und diese aktiviert ist.
- Auf dem Computer, mit dem Sie die Appliance verwalten, ist die Appliance nicht als dessen Proxy konfiguriert. Falls Sie zwischen dem Verwaltungscomputer und der Appliance einen Proxy haben, muss die Appliance als Übergabe-Host des Proxys konfiguriert werden.
- Falls Sie über den LAN1-Anschluss eine Remote-Verbindung zur Appliance über das Netzwerk haben, überprüfen Sie Folgendes:
  - Der verwendete Computer hat eine funktionstüchtige Verbindung zu Ihrem Netzwerk und kann dasselbe Subnetz erreichen, mit dem auch die Appliance verbunden ist.
  - Sie haben im URL-Feld des Webbrowsers die neue IP-Adresse verwendet, die Sie für den LAN1-Anschluss konfiguriert haben. Verwenden Sie die Standard-IP-Adresse 10.1.1.108, sofern Sie sie nicht deaktiviert oder gelöscht haben (https://10.1.1.108).

    Die IP-Adresse der Appliance muss für das Subnetz geeignet sein, mit dem die Appliance verbunden ist. Ist sie nicht geeignet, versuchen Sie es mit der Standard-IP-Adresse. Führt dies ebenfalls nicht zum Erfolg, versuchen Sie es über eine direkte Verwaltungsverbindung.

    HINWEIS: Über den LAN2-Anschluss erhalten Sie nur eine direkte Verwaltungsverbindung, wenn Sie die Appliance im Modus "Expliziter Proxy" verwenden und den LAN2-Anschluss nicht deaktiviert haben.

  - Die Appliance hat eine funktionierende Verbindung zu Ihrem vorhandenen Netzwerk, die durch die blinkende NIC-1-LED für Netzwerkaktivität in der Benutzeroberfläche angezeigt wird.

    Blinken die LEDs nicht, stellen Sie sicher, dass das verwendete Kabel unbeschädigt und ordnungsgemäß an den LAN1-Anschluss der Appliance sowie an Ihre vorhandenen Netzwerkgeräte angeschlossen ist. Falls Sie nicht das mit der Appliance gelieferte blaue Kabel verwendet haben, stellen Sie sicher, dass das Kabel ein durchgängiges (ungekreuztes) UTP-Netzwerkkabel ist.
- Wenn die Appliance im Modus "Expliziter Proxy" arbeitet und Sie eine direkte lokale Verwaltungsverbindung über den LAN2-Anschluss haben, überprüfen Sie Folgendes:
  - Der LAN2-Anschluss ist nicht deaktiviert. Stellen Sie eine Remote-Verbindung her, um dies zu überprüfen.

- Sie haben in das URL-Feld Ihres Webbrowsers die neue IP-Adresse eingegeben, die Sie für den LAN2-Anschluss konfiguriert haben (die Standardadresse lautet 10.1.2.108).
- Die Appliance hat eine funktionierende Verbindung zu Ihrem Computer, die durch die blinkende NIC-2-LED für Netzwerkaktivität im Bedienfeld angezeigt wird.

  Blinkt die LED nicht, stellen Sie sicher, dass das verwendete Kabel unbeschädigt und ordnungsgemäß an den LAN2-Anschluss der Appliance sowie an den Netzwerkanschluss Ihres Computers angeschlossen ist. Falls Sie nicht das mit der Appliance gelieferte orangefarbene Kabel verwendet haben, stellen Sie sicher, dass das Kabel ein gekreuztes UTP-Netzwerkkabel ist.

Mein Kennwort ist ungültig.

Wenn Sie kürzlich die Software der Appliance wiederhergestellt haben, ohne die vorherigen Einstellungen beibehalten zu haben, wird das Verwaltungskennwort auf das Standardkennwort **scmchangeme** zurückgesetzt.

Ich habe mein Kennwort vergessen.

Verwenden Sie die Wiederherstellungs-CD der Appliance, um das Kennwort der Appliance auf die Standardkennwörter scmchangeme und dlpchangeme zurückzusetzen.

Ein Teil der Benutzeroberfläche wird nicht korrekt angezeigt.

Die Benutzeroberfläche der Appliance ist für Internet Explorer 6.0 oder höher (unter Windows) sowie für Mozilla Firefox 2.0 (unter Linux) vorgesehen. Überprüfen Sie in den beigefügten Versionshinweisen, ob es bei der Verwendung einiger Webbrowser auf bestimmten Betriebssystemen Probleme gibt.

Clients (Software) können nicht über die Appliance kommunizieren.

Überprüfen Sie Folgendes:

- Die korrekten Protokolle für die Appliance sind aktiviert (standardmäßig sind alle Protokolle aktiviert).
- Die Clients und andere Geräte sind so konfiguriert, dass sie den Datenverkehr an die Appliance und von der Appliance leiten.
- Es bestehen keine Netzwerkprobleme, und Ihr Gerät ist ordnungsgemäß angeschlossen.

Webbrowsing funktioniert nicht, oder URL-Blockierung wird nicht durchgesetzt.

Die Appliance muss Zugriff auf einen DNS-Server haben, um Webbrowsing-Anfragen (über HTTP) überprüfen zu können und zu ermitteln, welche URLs blockiert werden sollen, falls das Blockieren von URLs konfiguriert ist.

E-Mail-Probleme

In diesem Abschnitt werden E-Mail-Probleme erläutert.

Anti-Relay funktioniert nicht.

So aktivieren Sie die Anti-Relay-Funktion:

1 Wählen Sie **E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Anti-Relay-Einstellungen**.

2 Fügen Sie mindestens eine lokale Domäne hinzu. Andernfalls ist die Appliance vor Weiterleitungen und Missbrauch durch Spammer von außerhalb Ihres Netzwerks ungeschützt.

Warum kann ich nicht nur den Namen des Absenders angeben, für den ich das Relay blockieren möchte?

Sie müssen sich das Anti-Relay als eine Blockierung zwischen zwei Systemen vorstellen, Anti-Spam hingegen als eine absenderbasierte Blockierung.

Das Anti-Relay wird mithilfe der Domänen und Netzwerke konfiguriert, für die die Appliance E-Mails überträgt. Die Anti-Spam-Konfiguration blockiert eine Nachricht jedoch basierend auf deren Absender.

Die Directory Harvest-Prävention funktioniert nicht.

Damit die Directory Harvest-Prävention ordnungsgemäß funktioniert, muss der E-Mail-Server während der SMTP-Kommunikation eine Überprüfung auf gültige Empfänger durchführen und anschließend einen Non-Delivery-Report senden.

Einige E-Mail-Server senden keine Fehler vom Typ "Unbekannter Benutzer" als Teil der SMTP-Konfiguration. Dazu gehören u. a. die folgenden Server:

- Microsoft Exchange 2000 und 2003 (wenn die Standardkonfiguration verwendet wird)
- qmail
- Lotus Domino

Schlagen Sie in der Benutzerdokumentation des E-Mail-Servers nach, ob der E-Mail-Server so konfiguriert werden kann, dass er den Bericht "550 Recipient address rejected: User unknown" (Empfängeradresse nicht akzeptiert: Unbekannter Benutzer) als Teil der SMTP-Kommunikation sendet, wenn eine Nachricht an einen unbekannten Benutzer gefunden wird.

Mit der LDAP-Integration kann dieses Problem umgangen werden. Weitere Informationen finden Sie im Produkthandbuch zu Ihrer Version der Email Security Appliance.

POP3

In diesem Abschnitt werden POP3-Probleme erläutert.

Ich habe eine dedizierte POP3-Verbindung eingerichtet, und POP3 funktioniert nicht mehr.

Der allgemeine und der dedizierte Server dürfen nicht denselben Port verwenden. Die Standard-Port-Nummer für POP3 lautet 110. Der dedizierte Server setzt den allgemeinen Server außer Kraft.

Wenn ich E-Mails mit Outlook Express über POP3 abrufe, erhalte ich manchmal eine Zeitüberschreitungsmeldung mit den Optionen "Abbrechen" oder "Warten".

Die Appliance muss die gesamte E-Mail-Nachricht herunterladen und scannen, bevor sie sie an Outlook Express weiterleiten kann. Bei einer großen Nachricht oder einem langsamen E-Mail-Server kann dies einige Zeit in Anspruch nehmen. Klicken Sie auf **Warten**, um Outlook Express zum Warten zu zwingen, bis die Appliance die Nachricht verarbeitet hat.

Ich erhalte gelegentlich POP3-Mail-Nachrichten doppelt.

Einige E-Mail-Clients gehen nicht korrekt mit Zeitüberschreitungen um. Wenn die Appliance eine sehr große Nachricht herunterlädt und scannt, kann beim Client während des Wartens auf eine Antwort eine Zeitüberschreitung eintreten.

Sie werden dann in einem Popup-Fenster aufgefordert, zu warten oder das Herunterladen abzubrechen. Wenn Sie **Abbrechen** wählen und einen zweiten Download starten, kann sich die Nachricht zwei Mal in Ihrem Posteingang befinden.

Probleme bei der physischen Konfiguration

In diesem Abschnitt werden Probleme mit der physischen Konfiguration erläutert.

In meinem Netzwerk sind zwei Appliances vorhanden, ich kann mich aber nur an einer anmelden.

Wenn Sie eine Appliance installiert oder kürzlich die Option "Konfiguration wiederherstellen" verwendet haben, ist es möglich, dass zwei oder mehr Appliances in Ihrem Netzwerk über die dieselbe Standard-IP-Adresse verfügen.

Um sicherzustellen, dass alle Appliances über eindeutige IP-Adressen verfügen, können Sie Folgendes verwenden:

- Den Setup-Assistenten
- Die Netzwerkeinstellungen
- Die Konfigurationskonsole

Probleme bei der automatischen Aktualisierung der Antiviren-Software

In diesem Abschnitt werden Probleme bei den automatischen Aktualisierungen der Antiviren-Software erläutert.

Wenn ich eine sofortige Aktualisierung anfordere, geschieht nichts. Wie kann ich erkennen, ob die DAT-Datei aktualisiert wurde?

So zeigen Sie die Versionsnummer der installierten DAT-Datei an:

- Wählen Sie im Dashboard im Bereich "Systemstatus" die Option **Aktualisierungen**.
- Wählen Sie alternativ **System | Komponentenverwaltung | Aktualisierungsstatus**.

Die DAT-Dateien werden heruntergeladen, geprüft und angewendet.

Die Appliance wartet nicht, bis die Aktualisierung vollständig durchgeführt worden ist (dies kann auch bei einer schnellen Internetverbindung einige Minuten dauern), sondern startet sie im Hintergrund.

Wählen Sie **System | Komponentenverwaltung | Aktualisierungsstatus**, um die neue DAT-Versionsnummer anzuzeigen, wenn Sie nach der Installation der neuen DAT-Dateien die Seite anzeigen.

Probleme mit Anti-Spam

In diesem Abschnitt werden Probleme mit dem Spam-Schutz erläutert.

Ich kann die in diesem Handbuch beschriebenen Anti-Spam-Funktionen nicht finden.

Für einige Anti-Spam-Funktionen muss das Anti-Spam-Modul aktiviert werden.

Ich habe die Appliance so konfiguriert, dass Spam-Mail durch eine RBL-Server-Überprüfung abgelehnt wird, aber einige Spam-Mails kommen dennoch an.

Es gibt keine Anti-Spam-Software, die sämtliche Spam-E-Mails erkennen und blockieren kann. Die Appliance verwendet eine Liste der Namen von bekannten Personen, die E-Mail-Missbrauch betreiben, sowie der von ihnen benutzten Netzwerke.

Diese Listen verringern die Anzahl unerwünschter E-Mails zwar wirksam, sind aber nicht vollständig.

So blockieren Sie einen bestimmten Spam-Absender:

1. Klicken Sie im Navigationsbereich auf **Konfigurieren | SMTP**.
2. Wählen Sie **Protokolleinstellungen | Einstellungen für Zulassen und Verweigern**.
3. Geben Sie unter **Absender verweigern** die E-Mail-Adresse des Absenders ein.

Benutzer erhalten keine regulären E-Mail-Nachrichten.

Benutzer empfangen möglicherweise aus folgenden Gründen keine regulären E-Mail-Nachrichten:

- Die E-Mail-Nachrichten könnten von einem Absender stammen, der in der Liste **Absender verweigern** aufgeführt ist. Sie müssen möglicherweise Folgendes durchführen:
  - Definieren Sie die Liste **Absender verweigern** genauer, um zu gewährleisten, dass erwünschte E-Mail-Nachrichten nicht blockiert werden. Es ist beispielsweise sinnvoller, eine bestimmte E-Mail-Adresse einzugeben, als eine gesamte Domäne oder ein gesamtes Netzwerk zu sperren.
  - Fügen Sie der Liste **Absender zulassen** den Absender, die Domäne oder das Netzwerk hinzu. Die Appliance scannt keine E-Mails von Absendern, Domänen und Netzwerken, die sich in dieser Liste befinden, auf Spam. Die Liste **Absender zulassen** hat Vorrang vor Einträgen in den Listen **Absender verweigern**.
- Die E-Mail-Nachricht wurde vielleicht blockiert, weil sie von einem Absender oder einem Unternehmen stammt, der bzw. das von einer Ihrer Echtzeit-Anti-Spam-Listen als potenzielle Spam-Quelle erkannt wurde.
- Das Verhältnis zwischen blockierten Spam- und regulären E-Mail-Nachrichten muss möglicherweise korrigiert werden. Wenn die Appliance beispielsweise selbst E-Mail-Nachrichten mit einem nur geringen Spam-Risiko blockiert, laufen Sie Gefahr, versehentlich auch normale E-Mail-Nachrichten zu blockieren. Es ist sinnvoller, eine gewisse Anzahl von Spam-Mails zu riskieren.
- Die E-Mail-Nachricht könnte einen Virus oder ein potenziell unerwünschtes Programm enthalten und wurde durch einen Virenscanner blockiert.

Benutzer erhalten weiterhin Spam.

Benutzer empfangen möglicherweise aus folgenden Gründen weiterhin Spam:

- Keine Anti-Spam-Software kann alle E-Mail-Nachrichten blockieren, die Spam enthalten könnten. Um Spam bestmöglich zu erkennen und zu verhindern, vergewissern Sie sich, dass die Appliance die neuesten Versionen des Anti-Spam-Moduls, der Anti-Spam-Regeln und zusätzlicher Regeldateien sowie alle Funktionen verwendet, die unerwünschte E-Mails blockieren können.
- Die Appliance lässt das Passieren von Stream-Medien zu.

  HINWEIS: Das Passieren von Stream-Medien stellt ein Sicherheitsrisiko dar, da Stream-Medien nicht von der Appliance gescannt werden. McAfee rät davon ab, Stream-Medien des Typs *application/octet-stream oder application/** die Appliance passieren zu lassen, da diese MIME-Typen ausführbar sind und ein hohes Sicherheitsrisiko darstellen.

- Die Anti-Spam-Erkennung ist nicht auf der Appliance aktiviert. Die Scan-Vorgänge müssen für die korrekte Richtung aktiviert werden. Wenn Spam aus einer externen Quelle erkannt werden soll, aktivieren Sie den Spam-Scan für eingehenden Datenverkehr. Wenn Spam aus einer internen Quelle erkannt werden soll, aktivieren Sie den Spam-Scan für ausgehenden Datenverkehr.
- Sie müssen möglicherweise eine strengere Anti-Spam-Richtlinie einrichten. Möglicherweise möchten Sie z. B. mehr E-Mail-Nachrichten als Spam markieren, bevor diese von den Benutzern empfangen werden, oder einfach Spam auf der Appliance-Ebene blockieren.
- Die E-Mail-Nachrichten könnten von Absendern, Domänen oder Netzwerken stammen, die in der Liste **Absender zulassen** aufgeführt sind. Überprüfen Sie die Liste, um sicherzugehen, dass E-Mail-Nachrichten von diesen Absendern wirklich vom Anti-Spam-Scan ausgenommen werden sollen. Möglicherweise sollten Sie die Einträge der Liste genauer definieren. Geben Sie beispielsweise einzelne E-Mail-Adressen an, statt ganze Domänen oder Netzwerke zuzulassen.
- Die E-Mail-Client-Software verschiebt unerwünschte Nachrichten nicht automatisch in einen Spam-Ordner. Benutzer sehen also weiterhin Spam-Nachrichten in ihrem Posteingang.
- Die E-Mail-Nachricht könnte größer sein als zulässig, weshalb sie nicht auf Spam gescannt wird. Die Größe können Sie in Ihren erweiterten Einstellungen für Spam ändern.
- Die E-Mail-Nachrichten werden nicht über eine Appliance geroutet, auf der das Anti-Spam-Modul aktiviert ist.

Wie kann ein bestimmter Typ von Spam gestoppt werden?

Überprüfen Sie Folgendes, um die optimale Erkennung und Vermeidung von Spam sicherzustellen:

- Die Appliance nutzt die neuesten Versionen des Anti-Spam-Moduls und der Anti-Spam-Regeln.
- Die Appliance wurde so konfiguriert, dass Stream-Medien die Appliance nicht passieren können.

Warum hat sich die Leistung verschlechtert?

Für das Scannen von E-Mail-Nachrichten auf Spam werden Ressourcen der Appliance benötigt, wodurch die SMTP-Leistung beeinträchtigt wird.

Benutzer klagen über volle Posteingänge.

Wenn Benutzer Spam automatisch in einen Spam-Ordner im Posteingang umleiten, kann ihr Posteingang rasch sein Größenlimit überschreiten. Erinnern Sie die Benutzer daran, regelmäßig ihre Spam-Ordner zu überprüfen und Spam zu löschen.

700-2959A15

McAfee®